

Commvault® MediaAgent on Cisco UCS C240 M5 Rack Server



This document provides an introduction to the process of deploying Commvault Data Platform on the Cisco UCS® C240 M5 Rack Server for a traditional Commvault MediaAgent architecture.

February 2018

Contents

- Introduction3
- Technology overview3
 - Cisco Unified Computing System.....3
 - Cisco UCS C240 M5 Rack Server5
 - Commvault® Data Platform5
 - Commvault® IntelliSnap® technology.....7
- Solution design and reference architecture configurations7
- Reference architecture.....8
 - Overview.....8
 - Storage capacity explained9
 - Individual MediaAgent server configurations.....9
- Cisco UCS C240 M5 configuration..... 11
 - Standalone configuration with Cisco Integrated Management Controller..... 11
 - Create virtual disk groups..... 18
 - Cisco UCS managed configuration with Cisco UCS Manager..... 22
 - Create a suborganization..... 27
 - Create the Cisco UCS C240 storage profile 28
 - Create disk group policies**..... 28
 - Create the boot disk group policy..... 28
 - Create the library disk group policy 31
 - Create the MediaAgent storage profile 32
 - Create the Cisco UCS C240 M5 server pool 35
 - Create boot policy..... 37
 - Create Microsoft Windows 40-Gbps adapter policy 39
 - Create a vNIC template..... 41
 - Create a service profile template..... 42
 - Create service profiles**..... 51
- OS installation for Commvault MediaAgent server..... 52
- Commvault MediaAgent installation and configuration..... 61
- For more information..... 63

Introduction

This document describes at a high level the installation and configuration steps for deploying the Commvault MediaAgent server on the Cisco UCS® C240 M5 Rack Server to build a data protection solution. This document does not provide a detailed step-by-step guide, and not every task is documented. The document focuses on the steps that are relevant to the specific use case under discussion. To complete the deployment, you should be familiar with the following:

- Cisco Unified Computing System™ (Cisco UCS) configuration
- Microsoft Windows installation and configuration
- Commvault® installation and configuration

Technology overview

This section introduces the technologies used in the solution described in this document.

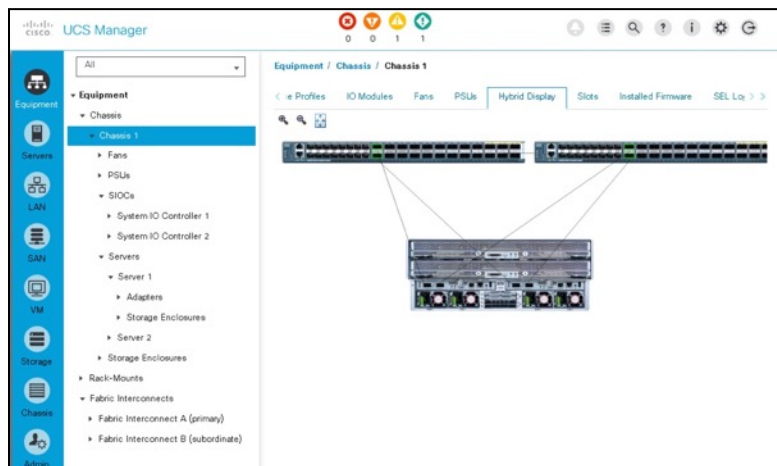
Cisco Unified Computing System

Cisco UCS is a state-of-the-art data center platform that unites computing, network, storage access, and virtualization resources into a single cohesive system.

The main components of Cisco UCS are described here:

- **Computing:** The system is based on an entirely new class of computing system that incorporates rack-mount and blade servers using Intel® Xeon® processor CPUs. The Cisco UCS servers offer the patented Cisco® Extended Memory Technology to support applications with large data sets and allow more virtual machines per server.
- **Network:** The system is integrated onto a low-latency, lossless, 10- or 40-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing (HPC) networks, which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- **Virtualization:** The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage access:** The system provides consolidated access to both SAN storage and network-attached storage (NAS) over the unified fabric. By unifying the storage access layer, Cisco UCS can access storage over Ethernet (with Network File System [NFS] or Small Computer System Interface over IP [iSCSI]), Fibre Channel, and Fibre Channel over Ethernet (FCoE). This approach provides customers with choice for storage access and investment protection. In addition, server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity and management for increased productivity.

Figure 1. Cisco UCS Manager



Cisco UCS consists of the following components:

- [Cisco UCS Manager](#) provides unified, embedded management of all Cisco UCS software and hardware components (Figure 1).
- [Cisco UCS 6000 Series Fabric Interconnects](#) are line-rate, low-latency, lossless, 10-Gbps Ethernet and FCoE interconnect switches providing the management and communication backbone for Cisco UCS.
- [Cisco UCS 5100 Series Blade Server Chassis](#) supports up to eight blade servers and up to two fabric extenders in a 6-rack unit (6RU) enclosure.
- [Cisco UCS B-Series Blade Servers](#) increase performance, efficiency, versatility, and productivity with Intel-based blade servers.
- [Cisco UCS C-Series Rack Servers](#) deliver unified computing in an industry-standard form factor to reduce total cost of ownership (TCO) and increase agility.
- [Cisco UCS S-Series Storage Servers](#) deliver unified computing in an industry-standard form factor to address data-intensive workloads with reduced TCO and increased agility.
- [Cisco UCS adapters](#), with wire-once architecture, offer a range of options to converge the fabric, optimize virtualization, and simplify management.

Cisco UCS is designed to deliver:

- Reduced TCO and increased business agility
- Increased IT staff productivity through just-in-time provisioning and mobility support
- A cohesive, integrated system that unifies the technology in the data center
- Industry standards supported by a partner ecosystem of industry leaders
- Unified, embedded management for easy-to-scale infrastructure

Cisco UCS C240 M5 Rack Server

The Cisco UCS C240 M5 Rack Server (Figure 2) is a 2-socket, 2RU rack server offering industry-leading performance and expandability. It supports a wide range of storage and I/O-intensive infrastructure workloads, including big data and analytics, data protection, and collaboration workloads. Cisco UCS C-Series Rack Servers can be deployed as standalone servers or as part of a Cisco UCS managed environment to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' TCO and increase business agility.

Figure 2. Cisco UCS C240 M5 Rack Server



In response to ever-increasing computing and data-intensive real-time workloads, the enterprise-class Cisco UCS C240 M5 server extends the capabilities of the Cisco UCS portfolio in a 2RU form factor. It incorporates the Intel Xeon Scalable processors, supporting up to 20 percent more cores per socket, twice the memory capacity, and five times more Non-Volatile Memory Express (NVMe) PCI Express (PCIe) solid-state disks (SSDs) than the previous generation of servers. These improvements deliver significant performance and efficiency gains that can improve your application performance. The C240 M5 delivers outstanding levels of storage expandability with exceptional performance, with:

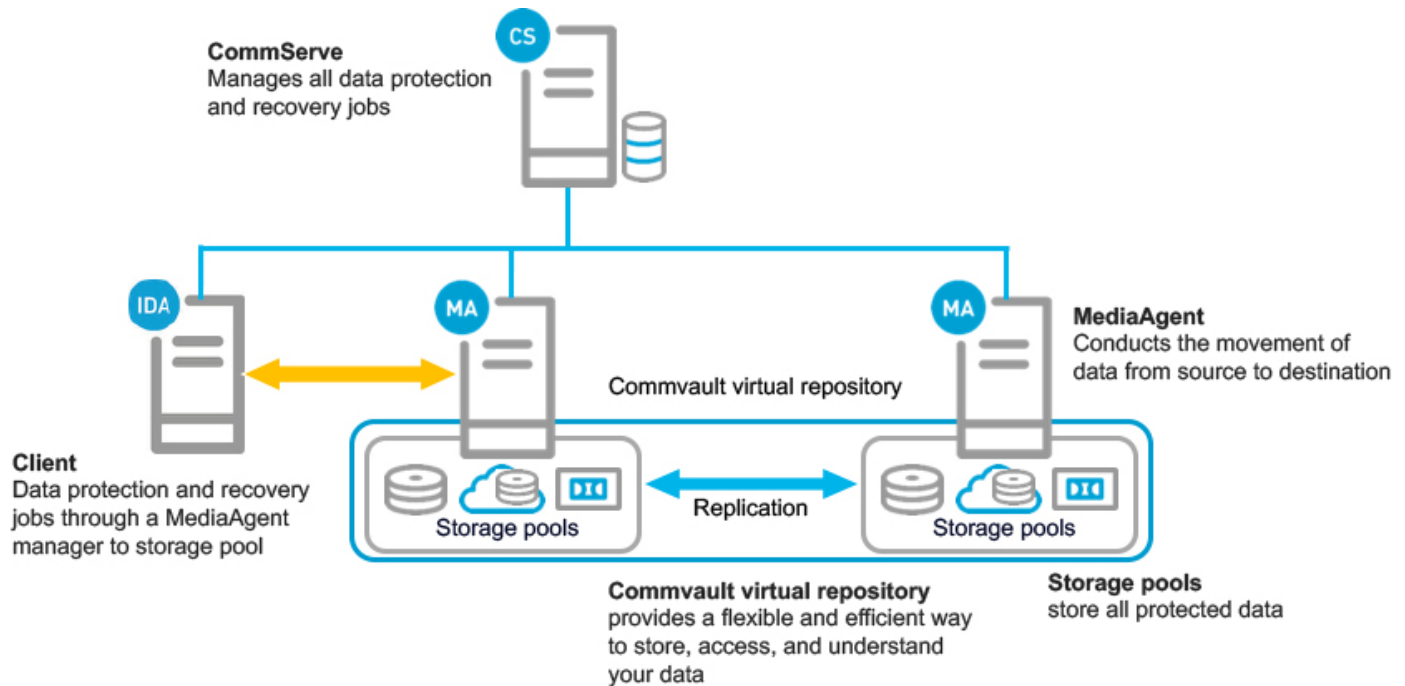
- The latest Intel Xeon Scalable CPUs, with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Intel 3D XPoint-ready support, with built-in support for next-generation nonvolatile memory technology
- Up to 26 hot-swappable small-form-factor (SFF) 2.5-inch drives, including 2 rear hot-swappable SFF drives (up to 10 support NVMe PCIe SSDs on the NVMe-optimized chassis version), or 12 large-form-factor (LFF) 3.5-inch drives plus 2 rear hot-swappable SFF drives
- Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- Modular LAN-on-motherboard (mLOM) slot that can be used to install a Cisco UCS virtual interface card (VIC) without consuming a PCIe slot, supporting dual 10- or 40-Gbps network connectivity
- Dual embedded Intel x550 10GBASE-T LAN-on-motherboard (LOM) ports
- Modular M.2 or Secure Digital (SD) cards that can be used for boot

Commvault® Data Platform

The Commvault Data Platform is a single platform for automated global protection, retention, and recovery. Commvault enterprise data protection and recovery software automates global data protection, accelerates recovery, reduces costs, and simplifies operations. Commvault integrates application awareness with hardware snapshots, indexing, global deduplication, replication, search, and reporting. The Commvault Data Platform converges all the needs of a modern data management solution in one place to seamlessly integrate protection, management, and access in one solution.

A comprehensive data protection and management strategy offers seamless and efficient backup, archiving, storage, and recovery of data in your enterprise from any operating system, database, and application. To protect and manage data in your environment, the Commvault software must be distributed to systems that you want to protect. CommServe®, MediaAgent, and protected systems constitute a CommCell® environment, and each protected system is referred to as a client (Figure 3).

Figure 3. Commvault Data Platform overview



The CommServe server is the command and control center of the CommCell architecture. It coordinates and runs all CommCell operations, maintaining Microsoft SQL Server databases that contain all configuration, security, and operational history for the CommCell environment. A CommCell environment can contain only one CommServe host. The CommServe software can be installed in physical, virtual, and clustered environments.

MediaAgent is the data transmission manager. It provides high-performance data movement and manages the data storage pools. When installed on a client system, it also manages the Commvault IntelliSnap snapshot integration with the underlying storage.

A client is any system within a CommCell environment to be protected. iDataAgents are software modules that are installed on computers to access and protect data. The backup and recovery system uses agents to interface with file systems, applications, and databases to facilitate the protection of data on production systems. By default, a file system iDataAgent module is installed when the Commvault software is added to a system. If the client hosts specific applications or databases, additional iDataAgents are required.

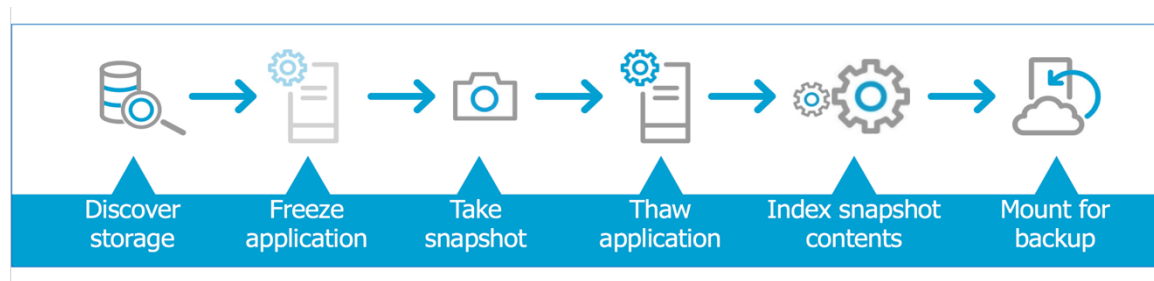
These three Commvault components combined offer the most comprehensive and flexible data protection solution on the market today.

Commvault® IntelliSnap® technology

IntelliSnap technology integrates with leading storage arrays, such as Pure Storage arrays, to provide consistent point-in-time recovery copies integrated into the data protection process. Unlike many other hardware-based copy management approaches, IntelliSnap extends beyond just creating or deleting snapshots. Snapshot contents are indexed to enable simple, specific object recovery, and snapshots can, for example, be mounted to allow the creation of a backup copy for a cloud library. Snapshots are integrated into virtual machine, database, and application protection schemes, enabling highly specific, partial, and point-in-time recovery operations from snapshot-based backup copies.

Figure 4 shows the snapshot creation process. Logically, it has six phases.

Figure 4. Six phases of the snapshot creation process



Solution design and reference architecture configurations

Commvault with Cisco UCS addresses the data protection needs of modern data centers. The increasing percentage of virtualized workloads, the dramatic increase in the size and amount of data, and the changes in the ways that companies do business and work with data have had an immense impact on data protection solutions. With the time requirement for backup operations reduced to minutes and the recovery point objective (RPO) and recovery time objective (RTO) requirements in the range of minutes to one hour, technologies such as compression, deduplication, replication, and backup to disk are essential in every design. The features and functions provided by Commvault, combined with the features and functions provided by Cisco UCS servers, create a powerful solution for fast backup and fast restore operations. For long retention periods and for less frequently accessed data, tape libraries or cloud storage can be used. With the combination of Cisco and Commvault technology, you can easily scale from tens of terabytes up to hundreds of petabytes (PB) of protected data.

Disks are now common backup media, and data backup on disk generally provides faster restore operations. Disk-based storage can be useful if you have many incremental backups and the percentage of data change is small. If the volume of data in incremental copies is insufficient to help ensure efficient writing to tape, consider disk storage. After writing the data to disk, you can use staging or storage lifecycle policies to copy batches of images to tape. This arrangement can produce faster backup operations and prevent wear and tear on your tape drives.

Consider the following factors when backing up a data set to disk or tape:

- Disks are well suited for short retention periods; tape is better suited for longer retention periods.
- Disks are well suited for staging; tape is good for long-term storage.
- Disks are better suited for low-volume incremental backups.
- Synthetic full backups are faster when incremental backup copies are stored on disk.

- Restoration from disk is usually faster than from tape.
- If client backup operations are too slow to keep the tape in motion, send the backups to disk.
- If the backups are small, send the backups to disk.
- Staging or lifecycle policies can later move the backup images to tape.

There is no “best” position in the infrastructure to install a Commvault with Cisco UCS solution. Many options are available regardless of how big a data center is. One option is to position the solution in a central place in the physical network so that it can be accessed from everywhere with the required bandwidth. Another option is to place the solution as close as possible to the data source.

With most data transferred from the backup client to the server and not directly from storage, and with the unique design of Cisco UCS, the use of a Cisco UCS domain will limit the network bandwidth required for data replication between the Commvault MediaAgent nodes. This option also allows Cisco UCS Manager to manage all Commvault MediaAgent servers in a central place.

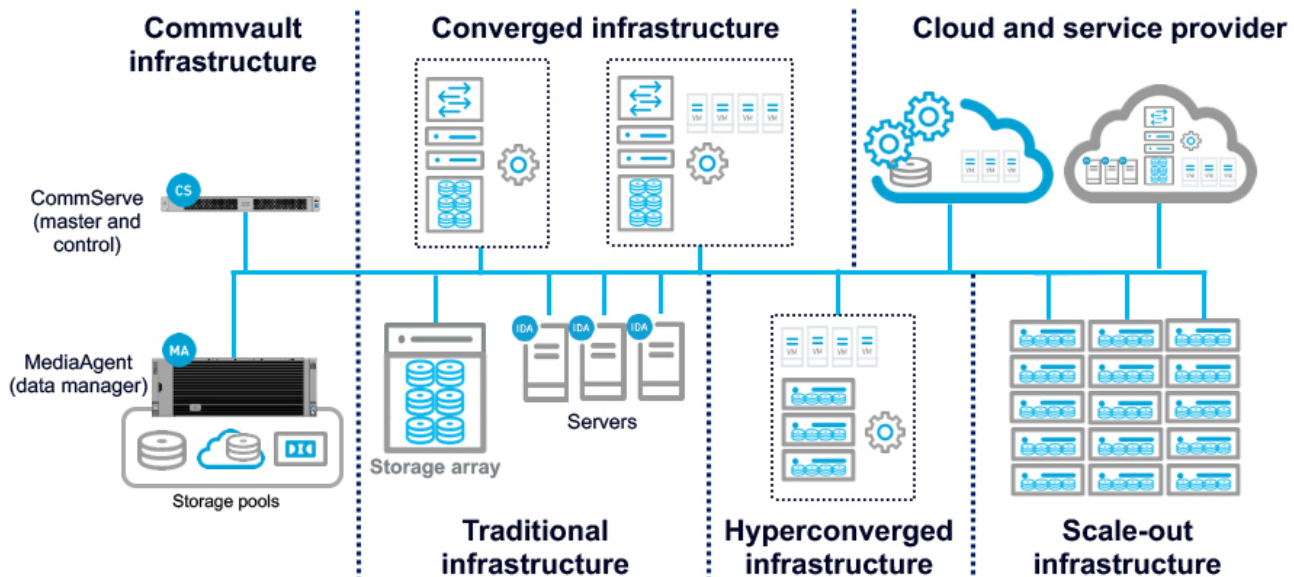
Reference architecture

This section introduces the reference architecture for the Commvault and Cisco solution.

Overview

Commvault and Cisco worked together to establish a simplified approach to sizing hardware to work within a Commvault environment. Building-block designs were aligned and tested with Commvault architecture deployments. This design is expandable from single-site to multisite, hybrid cloud, and public cloud environments, and any combination. Figure 5 shows the models and configuration needed for each size of Commvault MediaAgent. These models and configurations have been tested to provide the necessary requirements for each size. When ordering these approved and tested configurations, you can be assured of the proper performance.

Figure 5. Approved and tested configurations



Storage capacity explained

Customers sometimes ask why a freshly formatted hard disk or array is smaller than the advertised capacity. For example, a 1-TB drive has 931 GB after formatting.

The reason for this is that hardware and storage manufacturers count the capacity in different ways than the files system does. The prefixes kilo-, mega-, giga-, and tera- are used to state powers of ten. However, in computer software, the data being handled is typically organized based on powers of 2, so it became customary to call 2×10 a kilobyte, which is actually 1024 bytes, not exactly 1000 bytes.

There are prefixes to differentiate between base 10 and base 2; however, these are seldom used. In base 2 the proper terms are kibibyte, mebibyte, gibibyte, and tebibyte. The “bi” refers to binary, and the shortened terms are KiB, MiB, GiB, and TiB.

Here’s the underlying math:

- Hard disk manufacturers assume kilo = $10^3 = 1000$ (KB).
- File systems assume kilo = $2^{10} = 1024$ (KiB).

To convert KB, MB, and GB to KiB, MiB, and GiB, see the following list:

- KB to KiB: $1000/1024 = 0.9766$
- MB to MiB: $(1000 \times 1000) / (1024 \times 1024) = 0.9537$
- GB to GiB: $(1000 \times 1000 \times 1000) / (1024 \times 1024 \times 1024) = 0.9313$
- TB to TiB: $(1000 \times 1000 \times 1000 \times 1000) / (1024 \times 1024 \times 1024 \times 1024) = 0.9095$

Typically, software will display GB or TB as the storage unit, but the amount actually is Gib or TiB, so this confusion will remain unless this approach is changed.

Keep these values in mind as you review the Tables 1 and 2 in the next section. Capacities are stated using the sizes provided by the hardware manufacturer (base 10). Notes reference the software-based sizes (base 2).

Individual MediaAgent server configurations

Tables 1 and 2 summarize the individual MediaAgent server configurations available. You can choose a configuration based on your data protection requirements. This guide specifically focuses on Cisco UCS C240 as the MediaAgent server and uses a Small server in the example configuration. The storage configuration details depends on the specific customer environment and the size and number of drives available in the Cisco UCS C240 M5 server.

Table 1. Cisco Extra Small MediaAgent configuration

Commvault reference design: Cisco Extra Small MediaAgent configuration	
Cisco solution ID	Commvault MediaAgent XS C240
Cisco UCS server type	Cisco UCS C240 M5
Rack units	2RU (3.5 in. [88.9 mm])
Chip set	Intel C620 series
CPU type	1 x Intel Xeon Silver processor 4110 (2.1 GHz) <ul style="list-style-type: none"> • 16.8 GHz across 8 cores
Memory	2 x 8 DDR4 2400-MHz RDIMM (16 GB total)
Storage controller	12-Gbps modular SAS RAID controller with 2-GB cache

Commvault reference design: Cisco Extra Small MediaAgent configuration	
Storage: Boot plus metadata	2 x 960-GB SSD at 6 Gbps with RAID 1 (960 GB total*) <ul style="list-style-type: none"> • Access policy: Read-Write; read policy: No Read Ahead • Cache policy: Direct I/O; write policy: Write Through • Disk cache policy: Unchanged; stripe size: 64 KB • Index cache: 400 GB; deduplication database (DDB): 200 GB; and cloud copy DDB: 200 GB
Storage: Storage pool	7 x 4-TB near-line SAS (NL-SAS) with RAID 6 (16 TB total with 1 hot spare*) <ul style="list-style-type: none"> • Access policy: Read-write; read policy: Always Read Ahead • Cache policy: Direct I/O; write policy: Write Back Good Backup Battery Unit (BBU) • Disk cache policy: Unchanged; stripe size: 512 KB
Network options	2 x 10 Gbps onboard, 2 X 40 Gbps Cisco VIC**
Additional connectivity	
Power specifications	2 x 1050-watt (W) AC power supplies***

*When these drives are formatted, the OS will show capacities in base 2, so 960 GB will be approximately 894 GB, and 16 TB will be approximately 15 TB.

**A Cisco virtual interface card (VIC) must be connected to the Cisco UCS fabric interconnects in a Cisco UCS managed setup.

***For these configurations, power supplies and power cables must be ordered separately to accommodate different power requirements in different regions.

Table 2. Cisco Small MediaAgent configuration

Commvault reference design: Cisco Small MediaAgent configuration	
Cisco solution ID	Commvault MediaAgent Small C240
Cisco UCS server type	Cisco UCS C240 M5
Rack units	2RU (3.5 in. [88.9 mm])
Chip set	Intel C620 series
CPU type	<ul style="list-style-type: none"> • 2 x Intel Xeon Silver processor 4110 (2.1 GHz) • 33.6 GHz across 16 cores
Memory	2 x 16 DDR4 2400-MHz RDIMM (32 GB total)
Storage controller	12-Gbps modular SAS RAID controller with 2-GB cache
Storage: Boot plus metadata	<ul style="list-style-type: none"> • 2 x 1.6-TB SSD at 6 Gbps with RAID 1 (1.6 TB total *) • Access policy: Read-Write; read policy: No Read Ahead • Cache policy: Direct I/O; write policy: Write Through • Disk cache policy: Unchanged; stripe size: 64 KB • Index cache: 400 GB; DDB: 400 GB; and cloud copy DDB: 400 GB
Storage: Storage pool	<ul style="list-style-type: none"> • 12 x 4-TB NL-SAS with RAID 6 (36 TB total with 1 hot spare*) • Access policy: Read-Write, read policy: Always Read Ahead • Cache policy: Direct I/O; write policy: Write Back Good BBU • Disk cache policy: Unchanged; stripe size: 512 KB
Network options	2 x 10 Gbps onboard, 2 X 40 Gbps Cisco VIC**
Additional connectivity	
Power specifications	2 x 1050W AC power supplies**

*When these drives are formatted, the OS will show capacities in base 2, so 1.6 TB will be approximately 1.45 TB, and 36 TB will be approximately 32.7 TB.

**A Cisco VIC must be connected to the Cisco UCS fabric interconnects in a Cisco UCS managed setup.

***For these configurations, power supplies and power cables must be ordered separately to accommodate different power requirements in different regions

Cisco UCS C240 M5 configuration

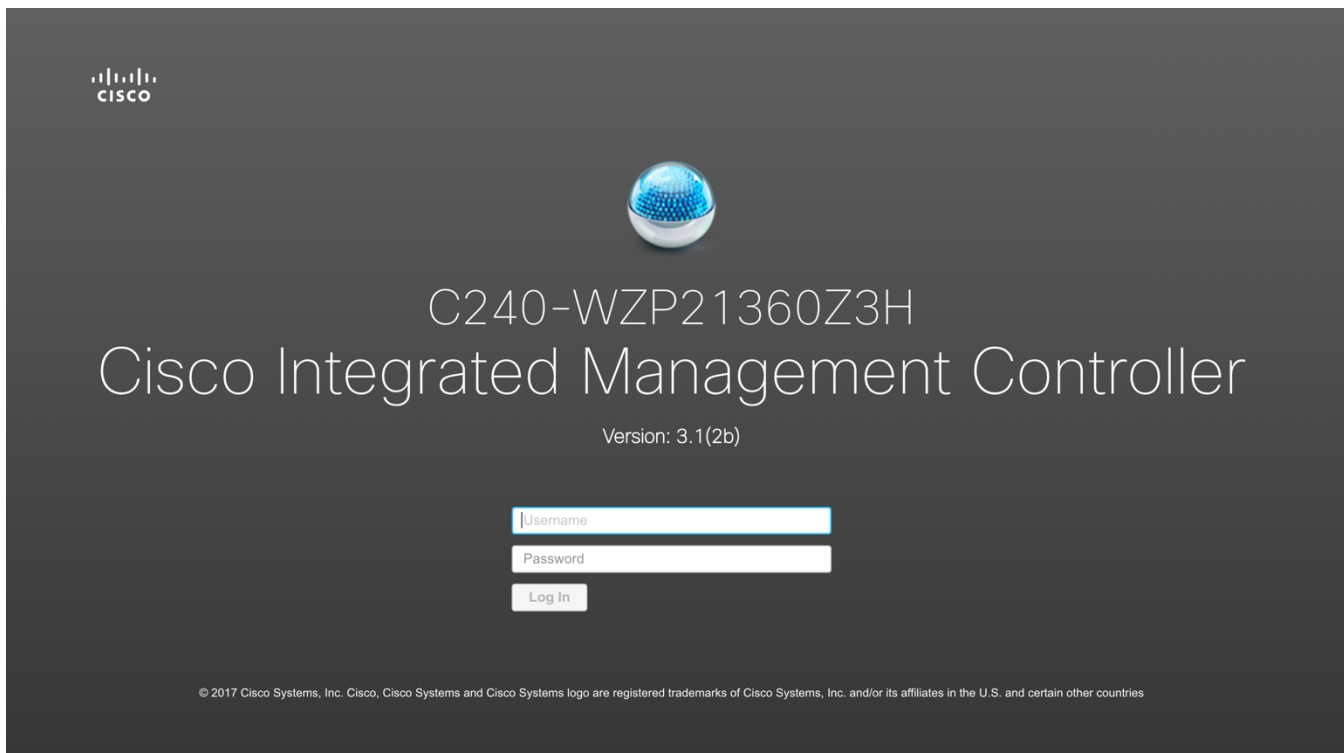
This document discusses the use of a standalone Cisco UCS C240 M5 Server as well as the use of a Cisco UCS C240 M5 Server managed by Cisco UCS to install Commvault MediaAgent server with a media management role.

Please use the Cisco UCS C240 M5 installation guide to complete the initial configuration (IP addresses, passwords, software versions, etc.). This document assumes that the C240 is accessible through the Cisco Integrated Management Controller (IMC) or Cisco UCS Manager over the network.

Standalone configuration with Cisco Integrated Management Controller

Follow these steps to configure a standalone solution using IMC.

1. Log on to the IMC as the admin user.



2. Check the condition of the system and the components required for the deployment on the Chassis > Summary page.

The screenshot shows the Cisco Integrated Management Controller (IMC) Chassis Summary page. The page is divided into two main sections: Server Properties and Cisco IMC Information.

Server Properties:

- Product Name: UCS C240 M5L
- Serial Number: WZP21360Z3H
- PID: UCSC-C240-M5L
- UUID: 6A9C4774-2C4A-41C7-8EBE-D87C7CCAD1C7
- BIOS Version: C240M5.3.1.2a.0.0918172340
- Description: [Empty text box]
- Asset Tag: [Unknown]

Cisco Integrated Management Controller (Cisco IMC) Information:

- Hostname: C240-WZP21360Z3H
- IP Address: 10.29.150.65
- MAC Address: 70:7D:B9:58:F2:30
- Firmware Version: 3.1(2b)
- Current Time (UTC): Tue Dec 19 15:24:43 2017
- Local Time: Tue Dec 19 15:24:43 2017 UTC +0000
- Timezone: UTC

Chassis Status:

- Power State: ● On
- Overall Server Status: ▼ Moderate Fault
- Temperature: ✔ Good
- Overall DIMM Status: ✔ Good
- Power Supplies: ▼ Fault
- Fans: ✔ Good
- Locator LED: ● Off
- Overall Storage Status: ✔ Good

Server Utilization:

- Overall Utilization (%): N/A
- CPU Utilization (%): N/A
- Memory Utilization (%): N/A
- IO Utilization (%): N/A

3. Choose Networking and Adapter Card to see the Cisco VIC configuration.
4. The General tab provides an overview of the adapter card and Ethernet ports, including the uplink status and port speeds.

The screenshot shows the Cisco IMC Adapter Card MLOM General configuration page. The page is divided into several sections:

General:

- Export vNIC | Import vNIC | Reset | Reset To Defaults

Adapter Card Properties:

- PCI-Slot: MLOM
- Vendor: Cisco Systems Inc
- Product Name: UCS VIC 1387
- Product ID: UCSC-MLOM-C40Q-03
- Serial Number: FCH21387A8J
- Version ID: V03
- Hardware Revision: 3
- Cisco IMC Management Enabled: no
- Configuration Pending: no
- ISCSI Boot Capable: True
- CDN Capable: True
- usNIC Capable: True
- Description: [Empty text box]
- Enable FIP Mode:
- Enable LLDP:
- Enable VNTAG Mode:
- Port-0: Auto
- Port-1: Auto

Firmware:

- Running Version: 4.2(2a)
- Backup Version: 4.2(2a)
- Startup Version: 4.2(2a)
- Bootloader Version: 4.2(2a)
- Status: Idle

External Ethernet Interfaces:

- Port-0:**
 - MAC Address: 38:0E:4D:B5:4A:4A
 - Link State: Link Down
 - Encap: CE
 - Admin Speed: Auto
 - Operating Speed: -
- Port-1:**
 - MAC Address: 38:0E:4D:B5:4A:4B
 - Link State: Link Down
 - Encap: CE
 - Admin Speed: Auto
 - Operating Speed: -

5. The virtual network interface cards (vNICs) tab summarizes the existing host Ethernet interfaces, including the maximum transmission unit (MTU) size, the uplink port used, and VLAN information. As a best practice, you should create at least one vNIC per uplink port or one vNIC per VLAN ID.

6. You should use MTU 9000 for the backup network if possible and on all participating devices in the network (clients, switches, and servers).

Host Ethernet Interfaces

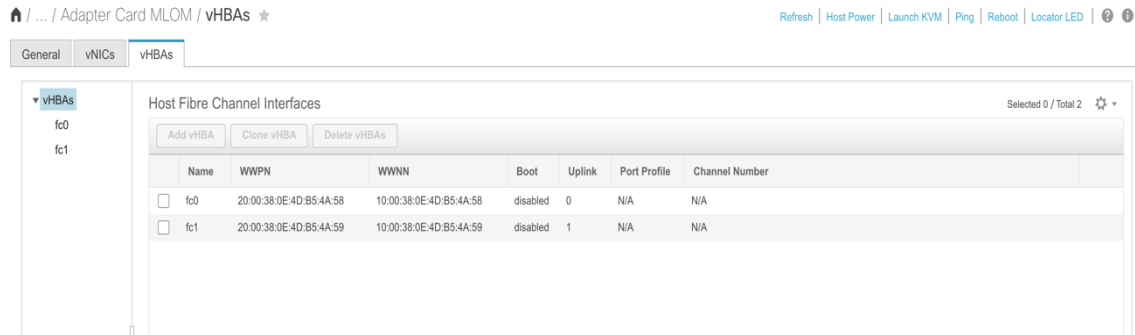
Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode	iSCSI Boot	PXE Boot	Channel	Port Profile	Uplink Failover
<input type="checkbox"/> eth0	VIC-MLO...	38:0E:4D:B5:4A:56	9000	0	0	0	NONE	TRUNK	disabled	disabled	N/A	N/A	N/A
<input type="checkbox"/> eth1	VIC-MLO...	38:0E:4D:B5:4A:57	9000	0	1	0	NONE	TRUNK	disabled	disabled	N/A	N/A	N/A

7. Click eth0 under vNICs in the left panel and set the following parameters to improve performance of Windows specific adapter with 40Gb NICs:
 - a. Transmit Queues: 8
 - b. Ring Size: 4096
 - c. Receive Queues: 8
 - d. Ring Size: 4096
 - e. Completion Queues: 16
 - f. Interrupts: 32
 - g. Receive Side Scaling (RSS): Enabled

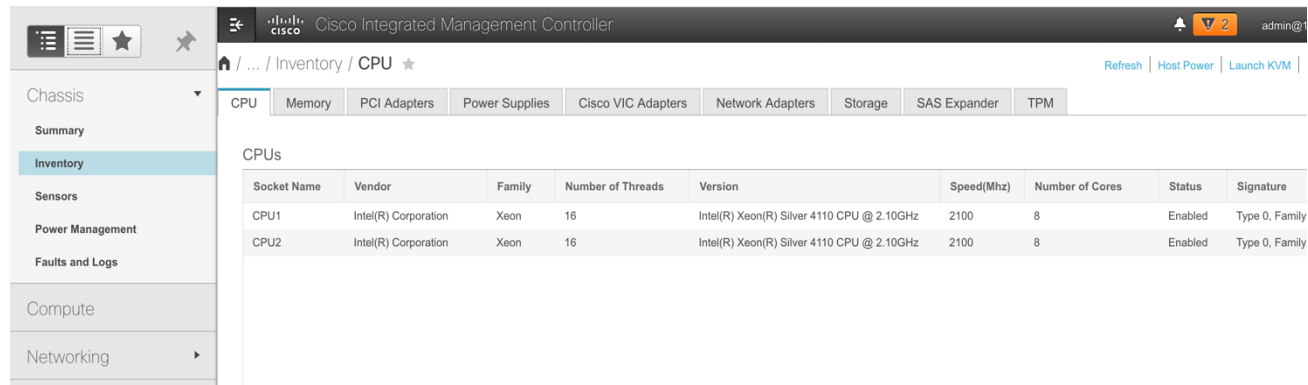
eth0 configuration details:

- Ethernet Interrupt:**
 - Interrupt Count: 32 (1 - 514)
 - Interrupt Mode: MSix
 - Coalescing Time: 125 (0-65535us)
 - Coalescing Type: MIN
- Ethernet Receive Queue:**
 - Receive Queue Count: 8 (1 - 256)
 - Receive Queue Ring Size: 4096 (64 - 4096)
- Ethernet Transmit Queue:**
 - Transmit Queue Count: 8 (1 - 256)
 - Transmit Queue Ring Size: 4096 (64 - 4096)
- Completion Queue:**
 - Completion Queue Count: 16 (1 - 512)
 - Completion Queue Ring Size: 1
- Receive Side Scaling:**
 - Enable TCP Receive Side Scaling:
 - Enable IP4 RSS:
 - Enable TCP-IP4 RSS:
 - Enable IP6 RSS:
 - Enable TCP-IP6 RSS:
 - Enable IP6 Extension RSS:
 - Enable TCP-IP6 Extension RSS:

8. Click Save Changes.
9. The virtual host bus adapter (vHBA) tab summarizes the existing host Fibre Channel Interfaces, including the worldwide port name (WWPN) and worldwide node name (WWNN) and information about whether the vHBA is used to boot the system. As a best practice, you should create at least one vHBA per uplink port or one vHBA per VSAN ID. Fibre Channel connectivity is used mainly for backup to Fibre Channel tape or for LAN-free backup directly from SAN storage.



10. The CPU tab of the Chassis Inventory pane shows the CPUs.



11. The Memory tab of the Chassis Inventory pane presents memory details.

Home / ... / Inventory / Memory

Refresh | Host Power | Launch KVM | Ping | Reboot | Locator LED

CPU | Memory | PCI Adapters | Power Supplies | Cisco VIC Adapters | Network Adapters | Storage | SAS Expander | TPM

Summary

Memory Speed	2400 MHz	Ignored Memory	0 MB
Total Memory	32768 MB	Number of Ignored DIMMs	0
Effective Memory	32768 MB	Number of Failed DIMMs	0
Redundant Memory	0 MB	Memory RAS Possible	MaximumPerformance Mirroring
Failed Memory	0 MB	Memory Configuration	MaximumPerformance

DIMM Black Listing

Overall DIMM Status ✔ Good

Enable DIMM Black List

[DIMM Location Diagram](#)

Memory Details Total 24 ⚙

Name	Capacity	Channel Speed (MHz)	Channel Type	Memory Type Detail	Bank Locator	Manufacturer	Serial Number	Asset Tag	Part Number	Visibility
DIMM_A1	8192 MB	2666	DDR4	Synchronous	NODE 1	0xCE00	03115527	CPU1_DIM...	M393A1G40EB2-CTD	Yes
DIMM_A2	Not Inst...	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIMM_B1	8192 MB	2666	DDR4	Synchronous	NODE 1	0xCE00	0311551C	CPU1_DIM...	M393A1G40EB2-CTD	Yes
DIMM_B2	Not Inst...	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIMM_C1	Not Inst...	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIMM_C2	Not Inst...	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIMM_D1	Not Inst...	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIMM_D2	Not Inst...	NA	NA	NA	NA	NA	NA	NA	NA	NA

12. The PCI adapters tab in the Chassis Inventory pane shows the PCIe adapter information such as the RAID controller and the Cisco VIC.

Home / ... / Inventory / PCI Adapters

Refresh | Host Power | Launch KVM | Ping | Reboot | Locator LED

CPU | Memory | PCI Adapters | Power Supplies | Cisco VIC Adapters | Network Adapters | Storage | SAS Expander | TPM

Slot ID	Product Name	Option ROM Status	Firmware Version	Vendor ID	Sub Vendor ID	Device ID	Sub Device ID
L	Ethernet Controller 10G X550T	Loaded	0x80000730-1.810.8	0x8086	0x1137	0x1563	0x01a4
MLOM	Cisco UCS VIC 1387 MLOM	Not Loaded	4.2(2a)	0x1137	0x1137	0x0042	0x015d
MRAID	Cisco 12G Modular RAID Controller with 2GB cache(M...	Loaded	N/A	0x1000	0x1137	0x0014	0x020e

13. The Storage tab of the Chassis Inventory pane shows the storage controller information.

Home / ... / Inventory / Storage

Refresh | Host Power | Launch KVM | Ping | Reboot | Locator LED

CPU | Memory | PCI Adapters | Power Supplies | Cisco VIC Adapters | Network Adapters | Storage | SAS Expander | TPM

Controller	PCI Slot	Product Name	Serial Number	Firmware Package Build	Product ID	Battery Status	Cache Memory Size	Health
MRAID	MRAID	Cisco 12G Modular Raid Controller ...	SK73065432	50.1.0-0726	LSI Logic	Optimal	0 MB	Good
SDHC	N/A	Cisco Flexutil	N/A	N/A	N/A	N/A	N/A	N/A

14. Double-click the Cisco 12G Modular Raid Controller product name.

The storage configuration is the most important part of the Cisco UCS C240 M5 configuration for the Commvault MediaAgent server.

15. The Storage pane shows the RAID controller information, physical drive and virtual drive information, and RAID settings.

Info ★

Controller Info	Physical Drive Info	Virtual Drive Info	Battery Backup Unit	Storage Log
<p>Health/Status</p> <p>Composite Health: ✔ Good</p> <p>Controller Status: Optimal</p> <p>RAID Chip Temperature: 60</p> <p>Storage Firmware Log Status: Not Downloaded</p>		<p>Settings</p> <p>Predictive Fail Poll Interval: 300 sec</p> <p>Rebuild Rate: 30 %</p> <p>Patrol Read Rate: 30 %</p> <p>Consistency Check Rate: 30 %</p> <p>Reconstruction Rate: 30 %</p> <p>Cache Flush Interval: 4 sec</p> <p>Max Drives To Spin Up At Once: 4</p> <p>Delay Among Spinup Groups: 6 sec</p> <p>Physical Drive Coercion Mode: 1 GB</p> <p>Cluster Mode: false</p> <p>Battery Warning: true</p> <p>ECC Bucket Leak Rate: 1440 min</p> <p>Expose Enclosure Devices: true</p> <p>Maintain PD Fail History: false</p> <p>Enable Copyback on SMART: true</p> <p>Enable Copyback to SSD on SMART Error: true</p> <p>Native Command Queuing: enabled</p> <p>JBOD: true</p> <p>Enable Spin Down of Unconfigured Drives: true</p> <p>Enable SSD Patrol Read: false</p> <p>AutoEnhancedImport: true</p>		
<p>Firmware Versions</p> <p>Product Name: Cisco 12G Modular Raid Controller with ?</p> <p>Serial Number: SK73065432</p> <p>Firmware Package Build: 50.1.0-0726</p>		<p>Capabilities</p> <p>HW Configuration</p> <p>Error Counters</p>		
<p>PCI Info</p> <p>PCI Slot: MRAID</p> <p>Vendor ID: 1000</p> <p>Device ID: 14</p> <p>Sub Vendor ID: 1137</p> <p>SubDevice ID: 20e</p>				
<p>Manufacturing Data</p> <p>Manufactured Date: 2017-07-28</p> <p>Revision: 08002</p>				
<p>Boot Drive</p> <p>Boot Drive: 6</p> <p>Boot Drive is PD: true</p>				
<p>Running Firmware Images</p> <p>Startup Firmware Images</p> <p>Virtual Drive Count</p> <p>Physical Drive Count</p>				

16. Click the Physical Drive Info tab.

Controller Info | **Physical Drive Info** | Virtual Drive Info | Battery Backup Unit | Storage Log

Physical Drives Selected 0 / Total 14

Make Global Hot Spare | Make Dedicated Hot Spare | Remove From Hot Spare Pools | Prepare For Removal | Undo Prepare For Removal | Enable JBOD | Set as Boot Drive

Controller	Physical Drive Number	Status	Health	Boot Drive	Drive Firmware	Coerced Size	Model	Type
<input type="checkbox"/>	MRAID 1	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 2	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 3	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 4	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 5	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 6	JBOD	Good	true	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 7	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 8	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 9	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 10	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 11	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 12	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 13	JBOD	Good	false	CS01	456809 MB	ATA	SSD
<input type="checkbox"/>	MRAID 14	JBOD	Good	false	CS01	456809 MB	ATA	SSD

17. In the Status column, the drives should be listed as Unconfigured Good. If they are not, select each drive one at a time and click Set State as Unconfigured Good at the upper right.

Controller Info | **Physical Drive Info** | Virtual Drive Info | Battery Backup Unit | Storage Log

Physical Drives Selected 1 / Total 14

Make Global Hot Spare | Make Dedicated Hot Spare | Remove From Hot Spare Pools | Prepare For Removal | Undo Prepare For Removal | **Set State as Unconfigured Good** | Set as Boot Drive

Controller	Physical Drive Number	Status	Health	Boot Drive	Drive Firmware	Coerced Size	Model	Type
<input checked="" type="checkbox"/>	MRAID 1	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 2	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 3	JBOD	Good	false	5703	3814697 MB	TOSHIBA	HDD

18. Configure the hot spare drive. This configuration has one hot spare (based on the Small MediaAgent configuration). Select physical drive 1 and click Make Global Hot Spare at the top of the list.

Controller Info | **Physical Drive Info** | Virtual Drive Info | Battery Backup Unit | Storage Log

Physical Drives Selected 1 / Total 14

Make Global Hot Spare | Make Dedicated Hot Spare | Remove From Hot Spare Pools | Prepare For Removal | Undo Prepare For Removal | Set State as JBOD | Set as Boot Drive

Controller	Physical Drive Number	Status	Health	Boot Drive	Drive Firmware	Coerced Size	Model	Type
<input checked="" type="checkbox"/>	MRAID 1	Unconfigured Good	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 2	Unconfigured Good	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 3	Unconfigured Good	Good	false	5703	3814697 MB	TOSHIBA	HDD
<input type="checkbox"/>	MRAID 4	Unconfigured Good	Good	false	5703	3814697 MB	TOSHIBA	HDD

19. In the Virtual Drive Info pane, no virtual drives should be listed. Remove any virtual drives that appear in this initial configuration.

Home / ... / Cisco 12G Modular Raid Controller with 2GB cache (max 16 drives) (MRAID) / **Virtual Drive Info** ★

Refresh | Host Power | Launch KVM | Ping | Reboot | Locator LED | ? | i

Controller Info | Physical Drive Info | **Virtual Drive Info** | Battery Backup Unit | Storage Log

Virtual Drives Selected 0 / Total 0 ⚙

Initialize | Cancel Initialization | Set as Boot Drive | Delete Virtual Drive | Edit Virtual Drive | Hide Drive | Secure Virtual Drive

Virtual Drive Number	Name	Status	Health	Size	RAID Level	Boot Drive

Create virtual disk groups

The following procedure creates two virtual disk groups, for the boot drive with RAID 1 and the disk library with RAID 6, for a Small MediaAgent configuration.

Create virtual disk groups 0 and 1.

1. On the Controller Info page, click Create Virtual Drive from Unused Physical Drives.

Home / ... / Cisco 12G Modular Raid Controller with 2GB cache (max 16 drives) (MRAID) / **Controller Info** ★

Refresh | Host Power | Launch KVM | Ping | Reboot | Locator LED | ? | i

Controller Info | Physical Drive Info | Virtual Drive Info | Battery Backup Unit | Storage Log

[Create Virtual Drive from Unused Physical Drives](#) |
 [Create Virtual Drive from an Existing Virtual Drive Group](#) |
 [Import Foreign Config](#) |
 [Clear Foreign Config](#) |
 [Clear Boot Drive](#) |
 [Get Storage Firmware Log](#) |
 [Enable Drive Security](#) |
 [Disable Drive Security](#) |
 [Clear Cache](#) |
 [Clear all Configuration](#) |
 [Set Factory Defaults](#) |
 [Switch to Remote Key Management](#) |
 [Switch to Local Key Management](#)

2. For the operating system and metadata, you must create a RAID 1 configuration on the two SSDs available in the chassis.
 - a. Select 1 as the RAID level.
 - b. Select physical drives 13 and 14 and add them to the drive group (click >>).
 - c. For the name, enter **Boot** (any other name can be used to identify the drive). Keep the default virtual drive parameters
 - d. Keep Cache Policy as Direct IO.
 - e. Keep Write Policy as Write Through.
 - f. Enter **456809** as the size and select MB as the unit (the size will vary for different capacity drives).
3. Click Create Virtual Drive.

Create Virtual Drive from Unused Physical Drives ? X

RAID Level: Enable Full Disk Encryption:

Create Drive Groups

Physical Drives Selected 0 / Total 12 ⚙

<input type="checkbox"/>	1	3814697 MB	TOSHIBA	HDD	SAS
<input type="checkbox"/>	2	3814697 MB	TOSHIBA	HDD	SAS
<input type="checkbox"/>	3	3814697 MB	TOSHIBA	HDD	SAS
<input type="checkbox"/>	4	3814697 MB	TOSHIBA	HDD	SAS
<input type="checkbox"/>	5	3814697 MB	TOSHIBA	HDD	SAS
<input type="checkbox"/>	6	3814697 MB	TOSHIBA	HDD	SAS

>>
<<

Drive Groups ⚙

	Name
<input type="checkbox"/>	DG [13.14]

Virtual Drive Properties

<p>Name: <input type="text" value="Boot"/></p> <p>Access Policy: <input type="text" value="Read Write"/></p> <p>Read Policy: <input type="text" value="No Read Ahead"/></p> <p>Cache Policy: <input type="text" value="Direct IO"/></p>	<p>Disk Cache Policy: <input type="text" value="Unchanged"/></p> <p>Write Policy: <input type="text" value="Write Through"/></p> <p>Strip Size (MB): <input type="text" value="64k"/></p> <p>Size: <input type="text" value="456809"/> <input type="text" value="MB"/></p>
---	--

4. Go to the Virtual Drive Info tab and select the Boot virtual drive.
5. Click Set as Boot Drive.

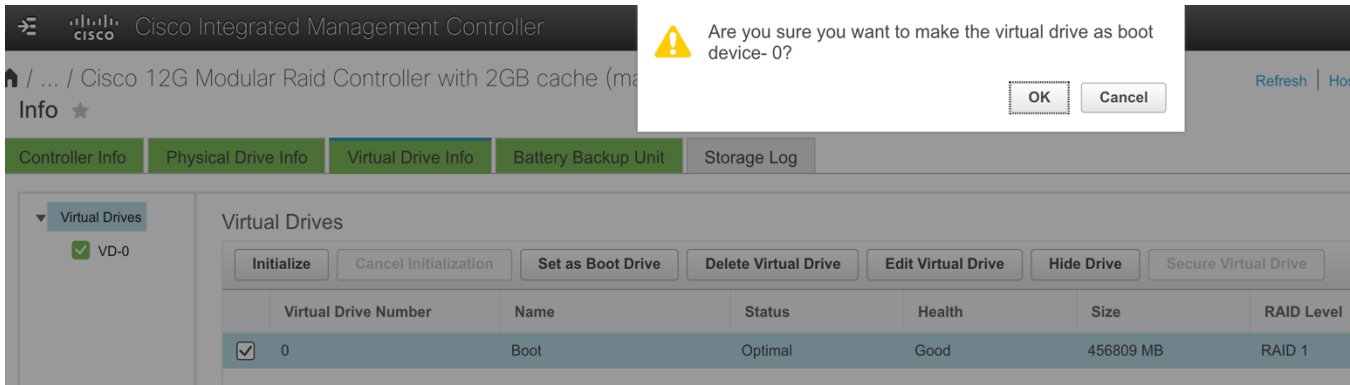
Home / ... / Cisco 12G Modular Raid Controller with 2GB cache (max 16 drives) (MRAID) / Virtual Drive Refresh | Host Power | Launch KVM | Ping | Reboot | Locator LED | ?

Info ★

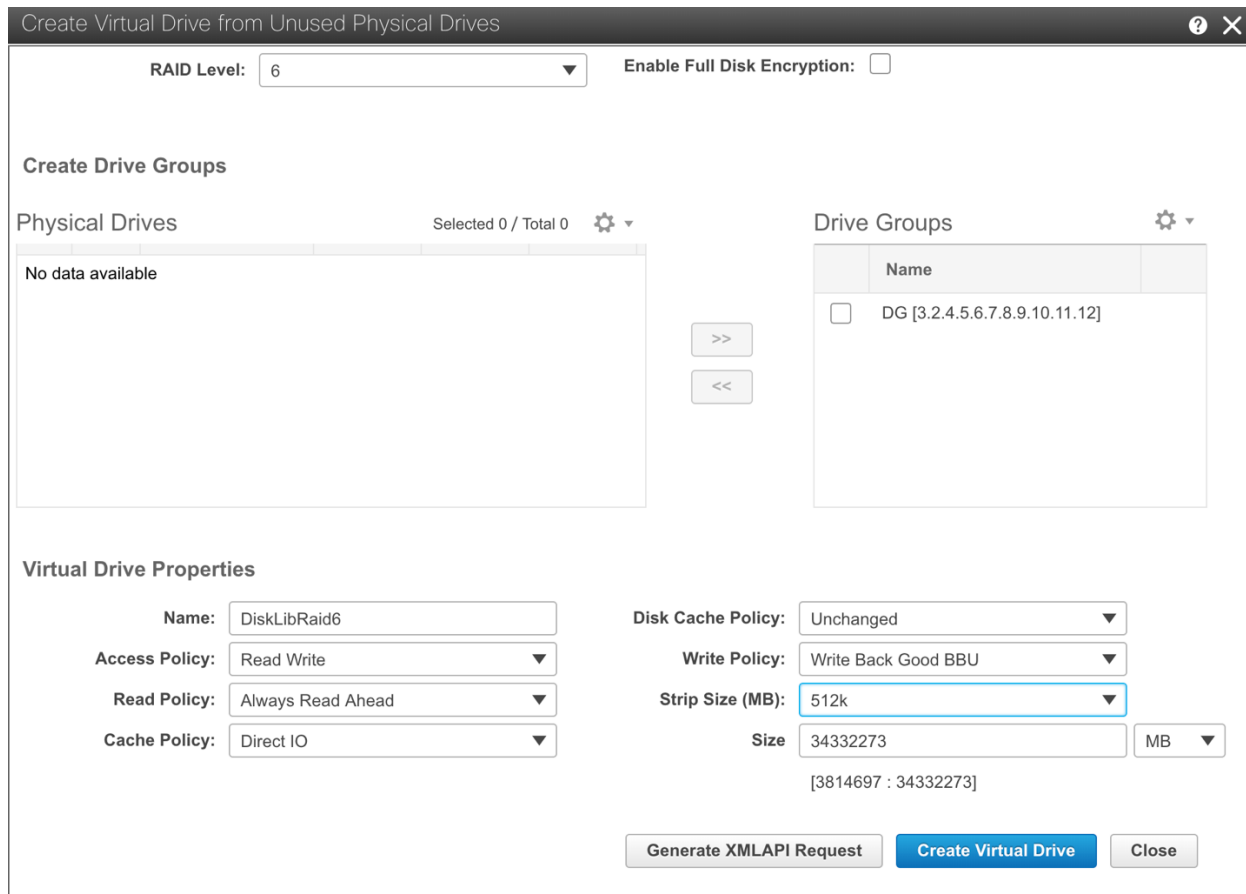
Virtual Drives Selected 1 / Total 1 ⚙

	Virtual Drive Number	Name	Status	Health	Size	RAID Level	Boot Drive
<input checked="" type="checkbox"/>	0	Boot	Optimal	Good	456809 MB	RAID 1	false

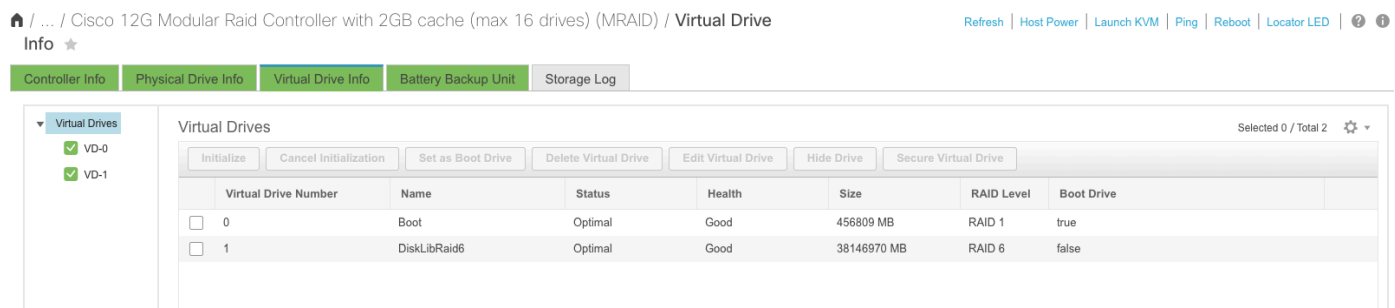
6. Confirm that you want to make the Boot virtual drive the boot drive.



7. Return to the Controller Info tab to create the additional virtual second drive group and virtual drive. The settings for the disk library described here are for the MediaAgent Small configuration, which uses 12 SAS drives.
8. Click Create Virtual Drive from Unused Physical Drives.
9. Select 6 as the RAID level.
10. Select physical drives 2 through 12 and add them to the drive group (click >>).

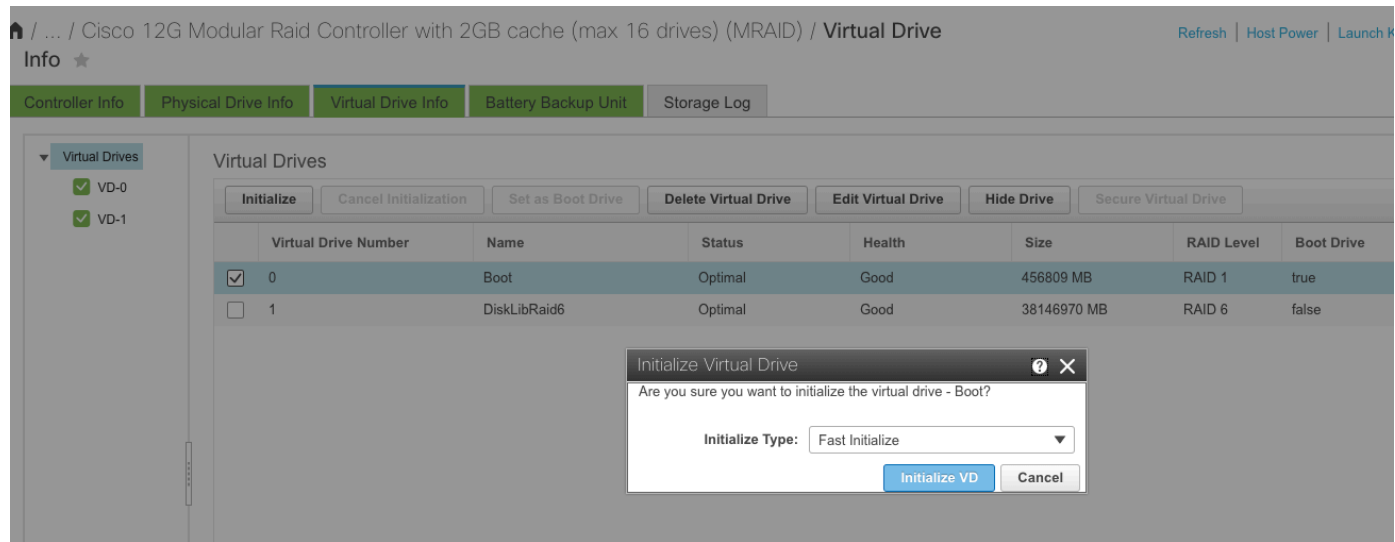


11. Provide the following values and complete the virtual drive creation process:
 - a. Enter **DiskLibRaid6** as the name (any other name can be used to identify the drive).
 - b. Change Read Policy to Always Read Ahead.
 - c. Change Cache Policy to Cached IO.
 - d. Change Write Policy to Write Back Good BBU.
 - e. Change Strip Size to 512 KB.
 - f. Use the size populated automatically or change the value to the maximum available space.
12. Click Create Virtual Drive.



Be aware that the disk group initialization process is ongoing in the background for several hours, and full performance is available only after the initialization process finishes.

13. Initialize the drives. Select a drive and click Initialize at the top left. In the next window, select Fast Initialize. Repeat this process for all drives.



14. To see the initialization progress, click the virtual drive in the left column (for example, VD-0).

▼ General

Name:	DiskLibRaid6	Consistency Check Operation Status:	Not Active
Strip Size:	512 KB	Requested Write Cache Policy:	Write Back Good BBU
Drives Per Span:	11	Current Write Cache Policy:	Write Back
Span Depth:	1	Disk Cache Policy:	Unchanged
Access Policy:	Read-Write	Allow Background Init:	true
Cache Policy:	Direct	Auto Snapshot:	false
Read Ahead Policy:	Always	Auto Delete Oldest:	true
Security Capable:	No	Boot Drive:	false
Security Enable:	No		

▼ Operation Status

Operation:	Foreground initialization in progress
Progress in %:	49
Elapsed Time (secs):	49

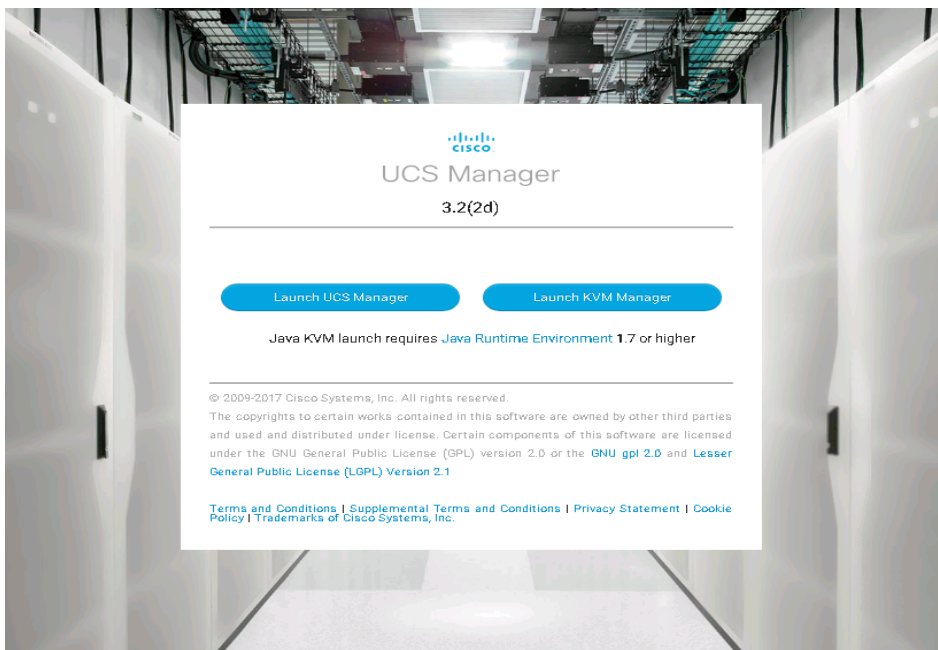
15. The server is now ready to load the OS.

Note: The number and size of drives dictate the virtual drive configuration. The values are based on the suggested MediaAgent configuration detailed earlier in this document.

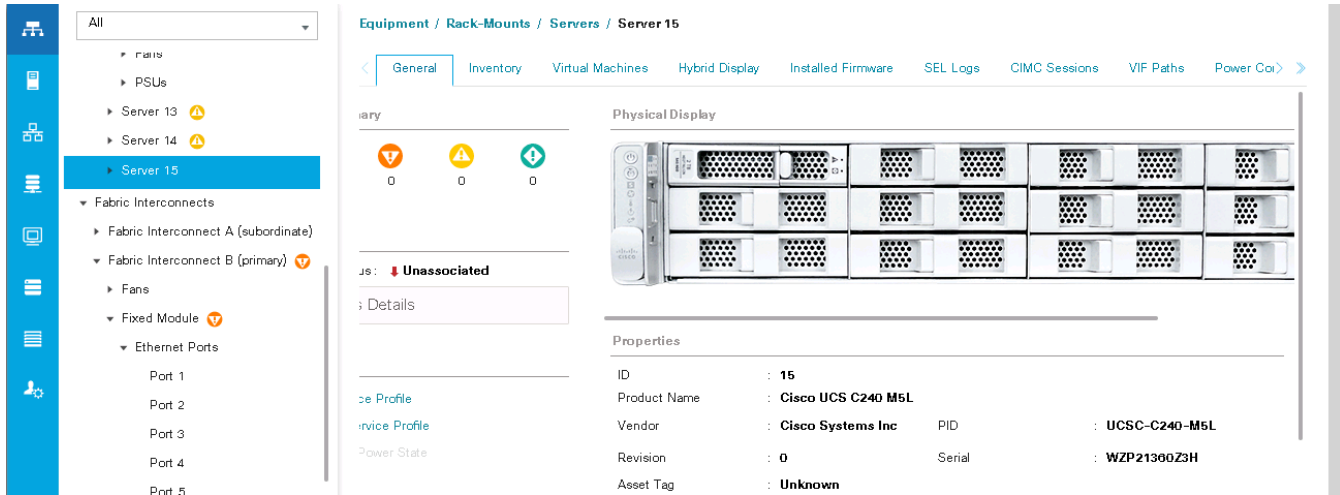
Cisco UCS managed configuration with Cisco UCS Manager

The following section covers the configuration of Cisco UCS managed Cisco C240 M5 servers.

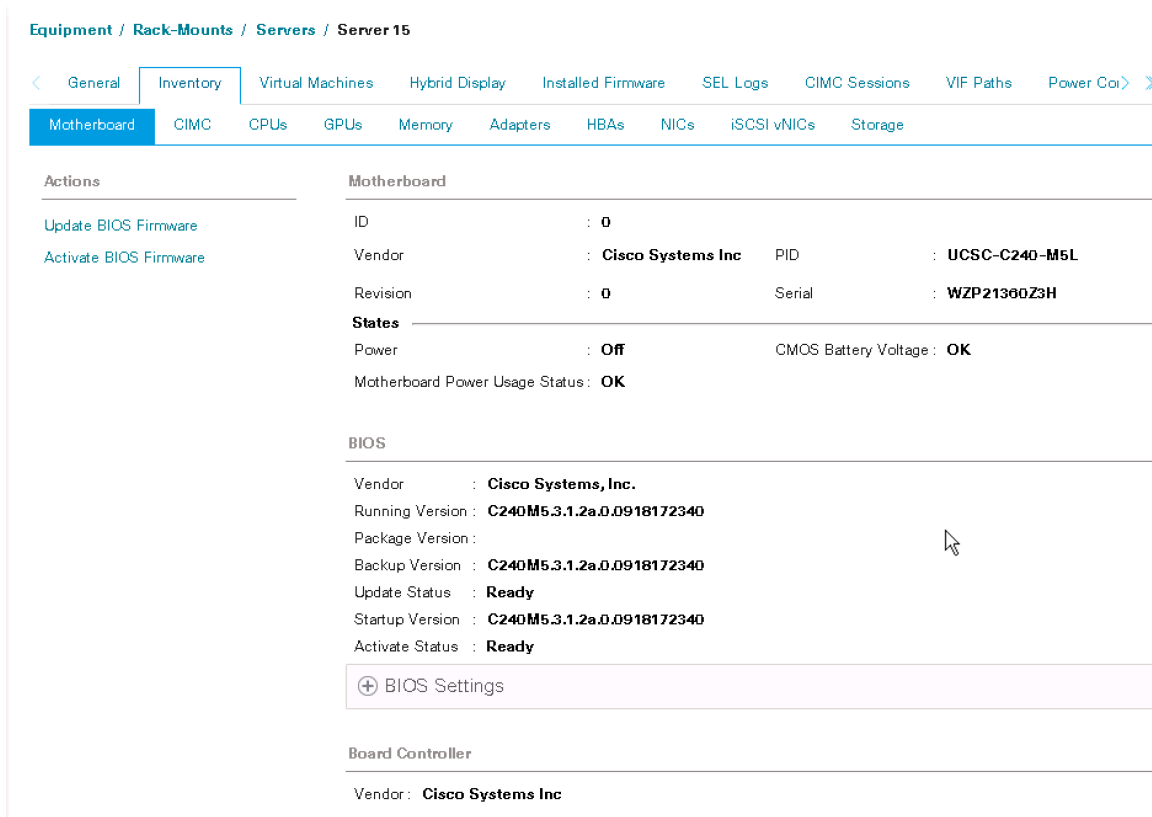
1. Log on to Cisco UCS Manager as the admin user or as another user with administrative rights.



- On the Equipment tab, identify the Cisco UCS C240 M5 server and verify the condition of the system and the components required for the deployment.



- Verify the server information. The Inventory tab shows the details of the server, including information about the CPU, memory, PCIe cards, and local storage.



Equipment / Rack-Mounts / Servers / Server 15

- General
 - Inventory
 - Virtual Machines
 - Hybrid Display
 - Installed Firmware
 - SEL Logs
 - CIMC Sessions
 - VIF Paths
 - Power Coi >
-
- Motherboard
 - CIMC
 - CPUs**
 - GPUs
 - Memory
 - Adapters
 - HBA's
 - NICs
 - iSCSI vNICs
 - Storage

Processor 1

Product Name	: Intel(R) Xeon(R) Silver 4110	Vendor	: Intel(R) Corporation
PID	: UCS-CPU-4110	Revision	: 0

[+ Part Details](#)

Processor Architecture	: Xeon		
CPU Stepping	: 4	Speed (GHz)	: 2.1
Socket Name	: CPU1	Number of Threads	: 16
Number of Cores	: 8	Number of Cores Enabled	: 8

States

Overall Status	: Operable	Power	: N/A
Operability	: Operable	Presence	: Equipped
Thermal	: OK		

Processor 2

Product Name	: Intel(R) Xeon(R) Silver 4110	Vendor	: Intel(R) Corporation
PID	: UCS-CPU-4110	Revision	: 0

[+ Part Details](#)

Processor Architecture: Xeon

Equipment / Rack-Mounts / Servers / Server 15

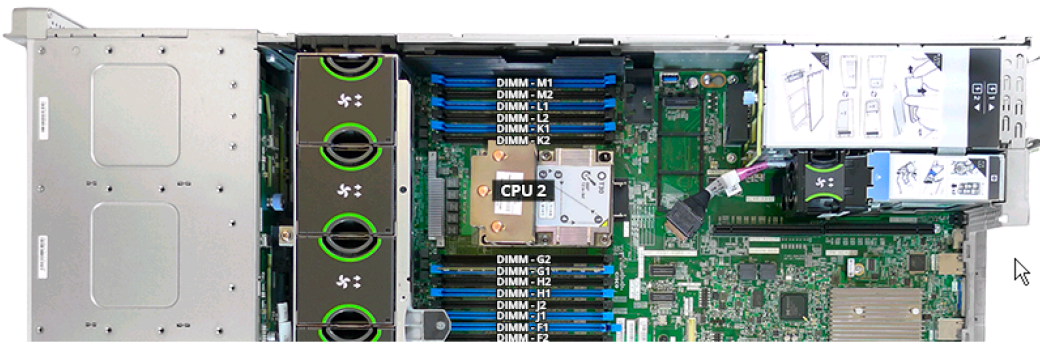
< General **Inventory** Virtual Machines Hybrid Display Installed Firmware SEL Logs CIMC Sessions VIF Paths Power Coi >

Motherboard CIMC CPUs GPUs **Memory** Adapters HBAs NICs iSCSI vNICs Storage

Advanced Filter Export Print

Name	Location	Capacity(GB)	Clock(MHz)
Memory 13	DIMM_G1	8.00	2666
Memory 3	DIMM_B1	8.00	2666
Memory 1	DIMM_A1	8.00	2666
Memory 15	DIMM_H1	8.00	2666
Memory 7	DIMM_D1	Unspecified	Unspecified
Memory 8	DIMM D2	Unspecified	Unspecified

+ Add - Delete Info



Save Changes Reset Values

Equipment / Rack-Mounts / Servers / Server 15

< General Inventory Virtual Machines Hybrid Display Installed Firmware SEL Logs CIMC Sessions VIF Paths Power Coi >

Motherboard CIMC CPUs GPUs Memory **Adapters** HBAs NICs iSCSI vNICs Storage

Advanced Filter Export Print

Name	Vendor	PID	Serial	Overall Status	Operability	Thermal
Adapter 1	Cisco Systems I...	UCSC-MLOM-C40Q-03	FCH21387A8J	N/A	N/A	N/A

- In a standalone configuration, the adapter includes predefined vNICs and vHBAs. In a configuration managed by Cisco UCS, however, nothing is defined. This definition is part of the service profile configuration. If PCIe cards for networking or Fibre Channel are installed, the information is listed on the NICs and HBAs tabs.

Equipment / Rack-Mounts / Servers / Server 15

< General **Inventory** Virtual Machines Hybrid Display Installed Firmware SEL Logs CIMC Sessions VIF Paths Power Coi >

Motherboard CIMC CPUs GPUs Memory Adapters HBAs **NICs** iSCSI vNICs Storage

+ - Advanced Filter Export Print

Name	vNIC	Vendor	PID	Model	Operability	MAC	Original MAC	ID
No data available								

Equipment / Rack-Mounts / Servers / Server 15

< General **Inventory** Virtual Machines Hybrid Display Installed Firmware SEL Logs CIMC Sessions VIF Paths Power Coi >

Motherboard CIMC CPUs GPUs Memory Adapters HBAs NICs iSCSI vNICs **Storage**

Controller LUNs Disks Security

+ - Advanced Filter Export Print

Name	ID	Type	Subtype
Storage Controller PCH 8	8	PCH	NA
Storage Controller SAS 1	1	SAS	NA
Storage Controller SATA 7	7	SATA	NA

General **Events**

Actions

No Actions Supported

Properties

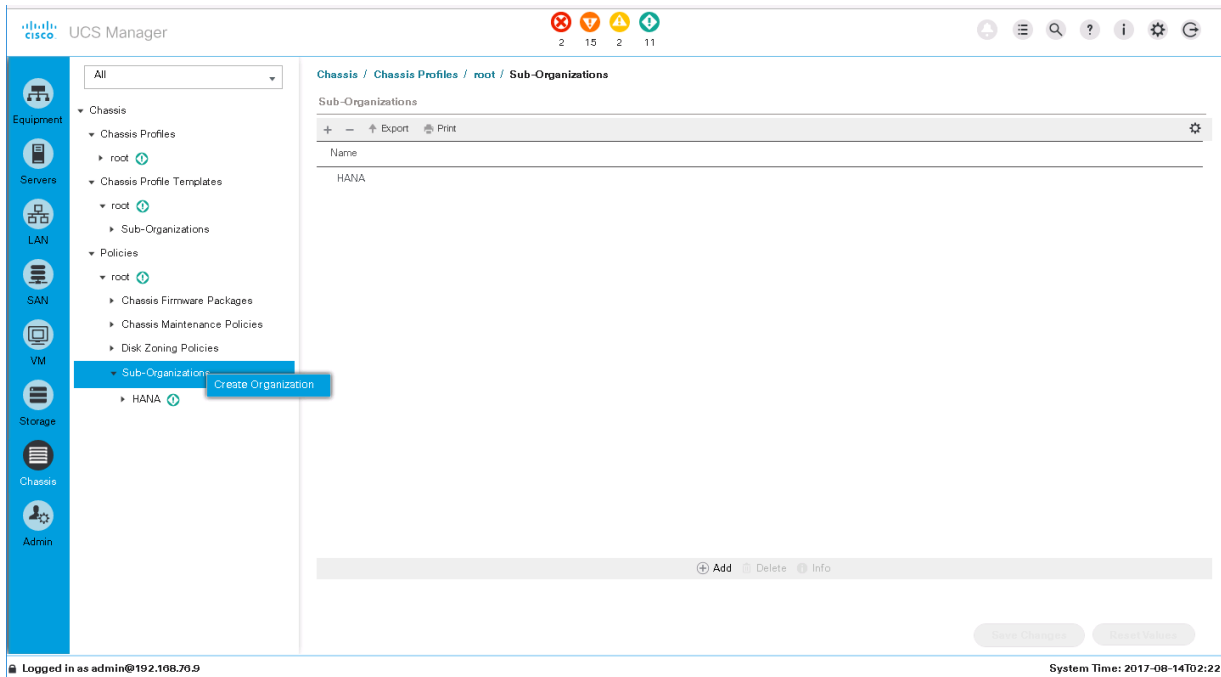
ID : **7** Subtype : **NA**
 Product Name : **Lewisburg PSATA Controller [SWRAID mode]**
 Vendor : **Intel Corp.** PID : **N/A**
 Revision : **0** Serial : **LSIROMB-0**

Part Details

Create a suborganization

The Cisco UCS Manager configuration for a Commvault MediaAgent server is specific to the use case. You can optionally define a new suborganization for Commvault to contain all configurations dedicated to this use case.

1. In the Chassis area, choose one of the root options and choose Sub-Organizations. Right-click and choose Create Organization.



2. Enter an obvious name such as **Commvault**, enter a description, and click OK.

Create Organization



Name :

Description :

Note: If you create a suborganization, you need to perform all the tasks described in the following steps, which are usually performed under the root organization, under the suborganization you created.

The next steps are dependent on the available disk drives C240 M5 Commvault MediaAgent server. To complete the storage configuration discussed earlier in this document, you need to identify the physical disks available for the operating system installation and disk library.

For a configuration with 12 disk drives for disk library, use the steps in the following sections.

Create the Cisco UCS C240 storage profile

The Cisco UCS C240 rack server will use a storage profile like the Cisco UCS S3260 Storage Server, but it will not need a controller definition, because the C240 in this environment has all disks in front-facing drive slots. You need to create two disk policies for local logical unit numbers (LUNs) to use as the boot device and the disk library for MediaAgent, and you can create others if additional local LUNs are needed.

The storage profile consists of storage policies used for creating local LUNs from the allocated disks (disk group policies).

Create disk group policies

You need to create two disk group policies for the MediaAgent deployment on the Cisco UCS C240 M5 based on the Small MediaAgent configuration options:

- **Boot_SSD1:** Boot plus metadata LUN for the SSD drives in a RAID 1 configuration
- **C240-Disk_Lib:** Disk library for MediaAgent using 12 HDDs with RAID 6 with 1 hot spare

Each of these disk group policies will create local LUNs for the C240 server, using available disks of specific types or manual slot specifications.

Create the boot disk group policy

To create the **Boot_SSD1** disk group policy, perform the following steps:

1. In Cisco UCS Manager, click **Storage** in the navigation pane and choose **Storage Policies** from the **Storage** pull-down menu options.
2. Right-click and choose **Create Disk Group Policy**.
3. Do the following:
 - a. Enter an appropriate name (**Boot_SSD1**).
 - b. Select **RAID 1 Mirrored**.
 - c. Select **Disk Group Configuration (Manual)**.
 - d. Click **Add** and enter **13** as the slot number.

Create Local Disk Configuration Reference

Slot Number : [1-205]

Role : Normal Dedicated Hot Spare Global Hot Spare

Span ID : [0-8]

4. Click OK.
5. Click Add again and enter **14** as the slot number.

Create Local Disk Configuration Reference

Slot Number : [1-205]

Role : Normal Dedicated Hot Spare Global Hot Spare

Span ID : [0-8]

6. Do the following:
 - e. Set Stripe Size to 64KB.
 - f. Set Access Policy to Read Write.
 - g. Set Write Cache Policy to Write Through.
 - h. Set IO Policy to Direct.
 - i. Set Drive Cache to No Change.

Create Disk Group Policy




Name :

Description :

RAID Level :

Disk Group Configuration (Automatic) Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Advanced Filter Export Print 

Slot Number	Role	Span ID
13	Normal	Unspecified
14	Normal	Unspecified

 Add  Delete  Info

Virtual Drive Configuration

Strip Size (KB) :

Access Policy : Platform Default Read Write Read Only Blocked

Create Disk Group Policy



Slot Number	Role	Span ID
13	Normal	Unspecified
14	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB) :

Access Policy : Platform Default Read Write Read Only Blocked

Read Policy : Platform Default Read Ahead Normal

Write Cache Policy : Platform Default Write Through Write Back Good Bbu Always Write Back

IO Policy : Platform Default Direct Cached

Drive Cache : Platform Default No Change Enable Disable

Security :

- Click OK to create the disk group policy.

Create the library disk group policy

To create the C240-Disk-Lib disk group policy, create a RAID 6 group with 11 drives and 1 hot spare.

- In Cisco UCS Manager, click Storage in the navigation pane and choose Storage Policies from the Storage pull-down menu options.
- Right-click and choose Create Disk Group Policy.
- Do the following:
 - Enter an appropriate name (**C240-Disk-Lib**).
 - Select RAID 6 Striped Dual Parity.
 - For Number of Drives, enter **11**.
 - Set Drive Type to HDD.
 - For Number of Dedicated Hot Spares, enter **1**.
 - Set Stripe Size to 512KB.
 - Set Read Policy to Read Ahead.
 - Set Write Cache Policy to Write Back Good Bbu.

Create Disk Group Policy



Name :

Description :

RAID Level :

Disk Group Configuration (Automatic)
 Disk Group Configuration (Manual)

Disk Group Configuration (Automatic)

Number of drives : **[0-60]**

Drive Type : Unspecified HDD SSD

Number of Dedicated Hot Spares : **[0-60]**

Number of Global Hot Spares : **[0-60]**

Min Drive Size (GB) : **[0-10240]**

Use Remaining Disks :

Use JBOD Disks : Yes No

Virtual Drive Configuration

Strip Size (KB) :

Access Policy : Platform Default Read Write Read Only Blocked

Read Policy : Platform Default Read Ahead Normal

Write Cache Policy : Platform Default Write Through Write Back Good Bbu Always Write Back

Write Cache Policy : Platform Default Write Through Write Back Good Bbu Always Write Back

IO Policy : Platform Default Direct Cached

Drive Cache : Platform Default No Change Enable Disable

Security :

- Click OK to create the disk group policy.

Create the MediaAgent storage profile

To create the MediaAgent storage profile, perform the following steps:

- In Cisco UCS Manager, click Storage in the navigation pane and choose Storage Profiles from the Storage pull-down menu options.
- Right-click and choose Create Storage Profile.
- Enter a name for the storage profile (**C240-MediaAgent**).

Create Storage Profile



Name :

Description :

LUNs

Local LUNs

Controller Definitions

Security Policy

⌵ Advanced Filter
⬆ Export
🖨 Print
⚙

Name	Size (GB)	Order	Fractional Size (MB)
No data available			

⊕ Add
🗑 Delete
ℹ Info



4. Select Add on the Local LUNs tab to add a LUN that will be created from the Boot_SSD1 disk group policy.
5. Specify the following in the Create Local LUN dialog box:
 - a. Enter a name (**Boot_SSD**).
 - b. Leave Size set to 1.
 - c. Leave Auto Deploy selected as Auto Deploy.
 - d. Select Expand To Available.
 - e. Choose the Boot_SSD1 disk group policy from the Select Disk Group Configuration pull-down menu.

Create Local LUN



Create Local LUN Prepare Claim Local LUN

Name :

Size (GB) : **[0-245760]**

Fractional Size (MB) :

Auto Deploy : Auto Deploy No Auto Deploy

Expand To Available :

Select Disk Group Configuration : [Create Disk Group Policy](#)

<not set>

Domain Policies

Boot_SSD1

C240-Disk-Lib

CV_Boot_Raid1

CV_Raid5DG_srv2

OK

Cancel

6. Click OK to add the local LUN.
7. Select Add on the Local LUNs tab to add a LUN that will be created from the C240-Disk-Lib disk group policy.
8. Specify the following in the Create Local LUN dialog box:
 - f. Enter a name (**Disk-Lib**).
 - g. Leave Size set to 1.
 - h. Leave Auto Deploy selected as Auto Deploy.
 - i. Select Expand To Available .
 - j. Choose the C240-Disk-Lib disk group policy from the Select Disk Group Configuration pull-down menu.

Create Local LUN



Create Local LUN
 Prepare Claim Local LUN

Name :

Size (GB) : **[0-245760]**

Fractional Size (MB) :

Auto Deploy : Auto Deploy No Auto Deploy

Expand To Available :

Select Disk Group Configuration : [Create Disk Group Policy](#)

<not set>

Domain Policies

Boot_SSD1

C240-Disk-Lib

CV_Boot_Raid1

CV_Raid5DG srv2

9. Click OK to add the local LUN.

10. Click OK to create the storage profile.

Create the Cisco UCS C240 M5 server pool

In addition to the storage profile, you need to create several new policies and pools before you can create for the C240 Server service profile. Existing pools and policies can be used if they are already created and can be used.

The C240 M5 server pool will contain C240 M5 servers to be used for MediaAgent. To create the server pool, follow these steps:

1. In Cisco UCS Manager, click Server in the Servers pane and choose Pools from the Server pull-down menu options.
2. Right-click Server Pools and choose Create Server Pool.
3. Enter an appropriate name for the server pool (**C240M5-MediaAgent**) and click Next.

Create Server Pool ? X

1 Set Name and Description

2 Add Servers

Name :

Description :

< Prev Next > Finish Cancel

4. The C240 M5 server was acknowledged in this environment as Server 15, so select 15, or the appropriate server numbers in your environment if they differ, and click the >> button between the Servers list and the Pooled Servers list.

Note: Select all the servers if you have more than one Cisco UCS C240 M5 server used as the MediaAgent server.

5. Click Finish to create the server pool.

Create boot policy

You need a boot policy to boot from the Boot_SSD1 local LUN created during the disk group policy portion of the storage profile creation process. To create the boot policy, follow these steps:

1. In Cisco UCS Manager, click Server in the navigation pane and choose Policies from the Server pull-down menu options.
2. Right-click Boot Policies under root and choose Create Boot Policy.
3. Enter a name for the policy (**C240-Boot_SSD**) and add a remote CD/DVD (used for KVM virtual media [vMedia] booting) under Local Devices.

Create Boot Policy



Name :

Description :

Reboot on Boot Order Change :

Enforce vNIC/vHBA/iSCSI Name :

Boot Mode : Legacy Uefi

WARNINGS:

The type (primary/secondary) does not indicate a boot order presence.
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
 If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Local Devices

- Add Local Disk
 - Add Local LUN
 - Add Local JBOD
 - Add SD Card
 - Add Internal USB
 - Add External USB
 - Add Embedded Local LUN
 - Add Embedded Local Disk
- Add CD/DVD
 - Add Local CD/DVD
 - Add Remote CD/DVD
- Add Floppy
 - Add Local Floppy

Boot Order

⚙️
+ - 🔍 Advanced Filter ↗️ Export 🖨️ Print

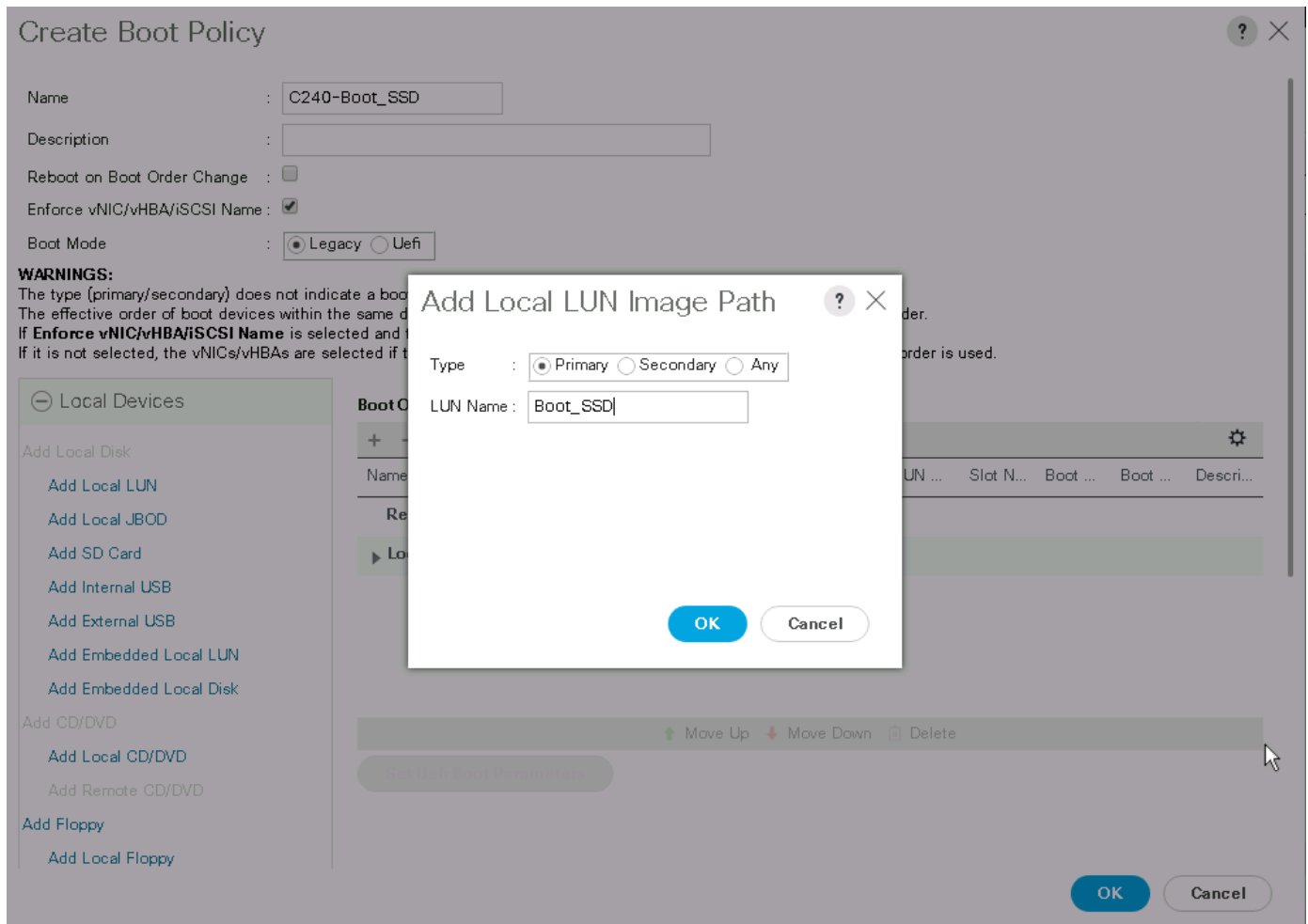
Name	Order▲	vNIC/v...	Type	WWN	LUN N...	Slot N...	Boot N...	Boot P...	Descri...
Remote CD/DVD	1								

⬆️ Move Up ⬆️ Move Down 🗑️ Delete

Set Default Boot Parameters

OK
Cancel

- Click Add Local LUN to reference the Boot_SSD LUN created by the Boot_SSD1 disk group policy.



5. Click OK and then click OK again to create the boot policy.

Create Microsoft Windows 40-Gbps adapter policy

You need to make some ring size adjustments and enable receive-side scaling for a Microsoft Windows-specific adapter for increased performance using 40-Gbps NICs. To create the adapter, follow these steps:

1. In Cisco UCS Manager, click Server in the navigation pane and choose Policies from the Server pull-down options.
2. Right-click Adapter Policies and choose Create Ethernet Adapter Policy.
3. Provide a name (**Windows-40G**) for the adapter policy and specify the following options:
 - h. Transmit Queues: 8
 - i. Ring Size: 4096
 - j. Receive Queues: 8
 - k. Ring Size: 4096
 - l. Completion Queues: 16

m. Interrupts: 32

n. Receive Side Scaling (RSS): Enabled

Create Ethernet Adapter Policy



Name :

Description :

Resources

Transmit Queues : [1-1000]

Ring Size : [64-4096]

Receive Queues : [1-1000]

Ring Size : [64-4096]

Completion Queues : [1-2000]

Interrupts : [1-1024]

Options

Transmit Checksum Offload : Disabled Enabled

Receive Checksum Offload : Disabled Enabled

TCP Segmentation Offload : Disabled Enabled

TCP Large Receive Offload : Disabled Enabled

Receive Side Scaling (RSS) : Disabled Enabled

Accelerated Receive Flow Steering : Disabled Enabled

Network Virtualization using Generic Routing Encapsulation : Disabled Enabled

OK

Cancel

4. Click OK to create the adapter policy

Create a vNIC template

MediaAgent can use the LAN connectivity policy and vNIC templates in the Cisco UCS domain, but only the in-band management network is needed. Other vNICs would not be used by the Windows OS. You can also set up A-B fabric failover in a new vNIC template, which will save you from having to configure NIC teaming in the Windows OS.

To create a vNIC template that will be used by MediaAgent, perform the following steps:

1. In Cisco UCS Manager, click LAN in the navigation pane and choose Policies from the Network pull-down menu options.
2. Right-click vNIC Templates under the root organization and choose Create vNIC Template.
3. Enter a name for the vNIC template and set the following options:
 - a. Fabric ID: Enable Failover
 - b. Template Type: Updating Template
 - c. VLANs: IB-Mgmt with Native VLAN selected

Create vNIC Template ? X

Name :

Description :

Fabric ID : Fabric A Fabric B Enable Failover

Redundancy

Redundancy Type : No Redundancy Primary Template Secondary Template

Target

Adapter VM

Warning

If **VM** is selected, a port profile by the same name will be created.
 If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : Initial Template Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print ⚙

Select	Name	Native VLAN
<input checked="" type="checkbox"/>	IB_MGMT	<input checked="" type="radio"/>
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	cvhci_vlan20	<input type="radio"/>

4. Scroll down to the second half of the window and select these additional options:

- d. MAC Pool: MAC_Pool_A
- e. Network Control Policy: Enable_CDP.

Note: The setup described here uses an existing predefined MAC address pool. Create a MAC address pool if you have a new installation of the Cisco UCS domain.

Create VLAN

CDN Source : vNIC Name User Defined

MTU : 1500

MAC Pool : MAC_A(26/64) ▼

QoS Policy : <not set> ▼

Network Control Policy : Enable_CDP ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

Connection Policies

OK

Cancel

2. Click OK to create the vNIC template.

Note: You should use MTU 9000 for the backup network if possible if this value is supported on all participating devices in the network (clients, switches, and servers).

Create a service profile template

With the storage profile ready and the vNIC template prepared, you can create the service profile template.

1. In Cisco UCS Manager, click Servers in the navigation pane and choose Service Profile Templates from the Server pull-down menu options.
2. Right-click root and choose Create Service Profile Template to open the Create Service Profile Template wizard.
3. Enter an appropriate name (**C240-MediaAgent**) for the service profile template.
4. Select the Updating Template option.
5. Under UUID, select UUID_Pool.

Note: The setup described here uses an existing predefined UUID pool. Create a UUID pool if you have a new installation of the Cisco UCS domain.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11

- Identify Service Profile Template
- Storage Provisioning
- Networking
- SAN Connectivity
- Zoning
- vNIC/vHBA Placement
- vMedia Policy
- Server Boot Order
- Maintenance Policy
- Server Assignment
- Operational Policies

Create Service Profile Template ? X

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.

Name :

The template will be created in the following organization. Its name must be unique within this organization.
Where : **org-root/org-Commvault**

The template will be created in the following organization. Its name must be unique within this organization.
Type : Initial Template Updating Template

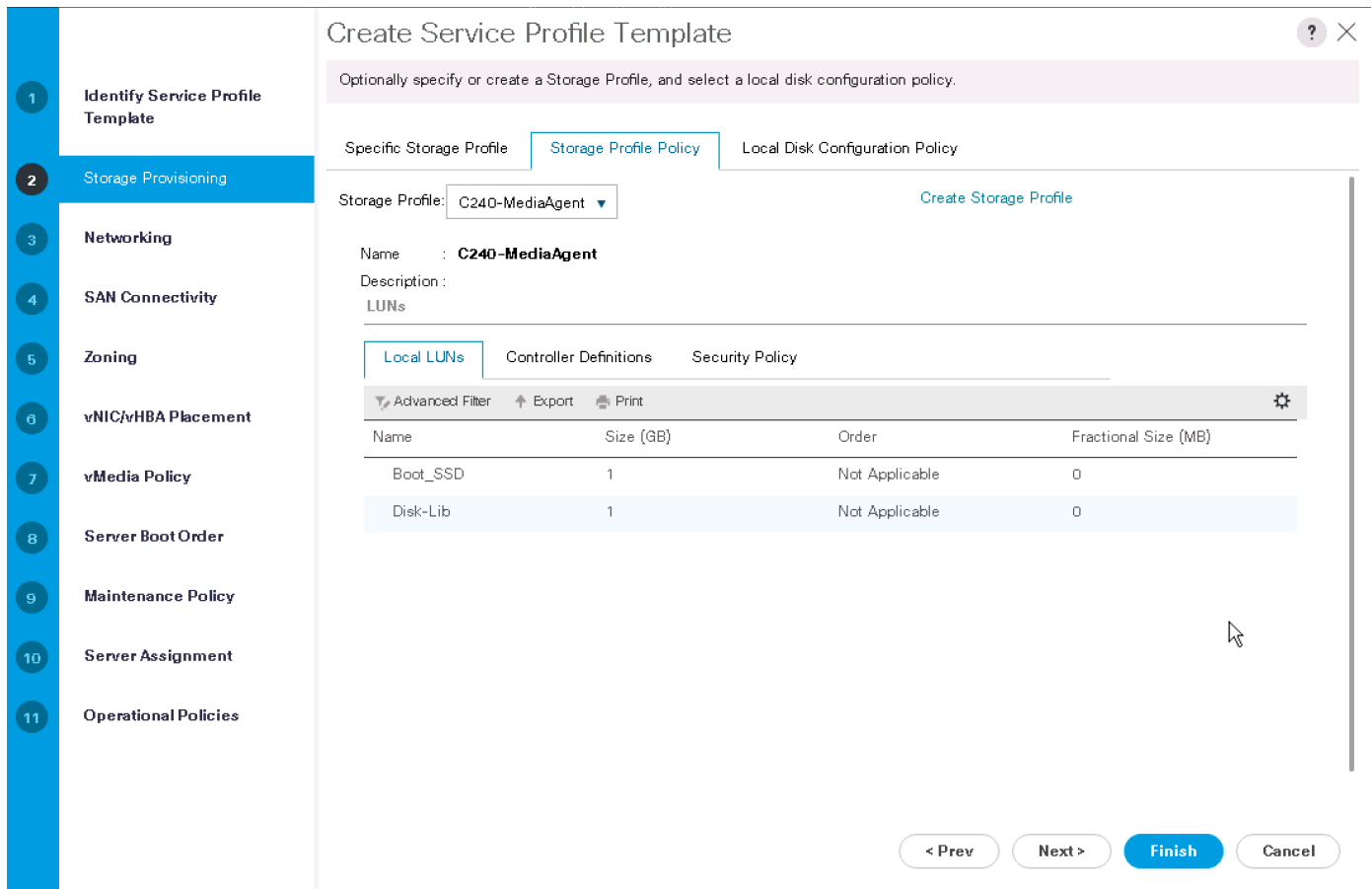
Specify how the UUID will be assigned to the server associated with the service generated by this template.
UUID

UUID Assignment:

The UUID will be assigned from the selected pool.
The available/total UUIDs are displayed after the pool name.

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

6. Click Next.
7. You move to the Storage Provisioning section. Click the Storage Profile Policy tab in the Storage Provisioning section and select the storage profile you previously created (C240-MediaAgent).



Create Service Profile Template

Optionally specify or create a Storage Profile, and select a local disk configuration policy.

Specific Storage Profile | **Storage Profile Policy** | Local Disk Configuration Policy

Storage Profile: C240-MediaAgent Create Storage Profile

Name : **C240-MediaAgent**
Description : LUNs

Local LUNs | Controller Definitions | Security Policy

Advanced Filter | Export | Print

Name	Size (GB)	Order	Fractional Size (MB)
Boot_SSD	1	Not Applicable	0
Disk-Lib	1	Not Applicable	0

< Prev | Next > | **Finish** | Cancel

8. Click Next.
9. You move to the Networking section, where you configure the network. Keep the default setting for Dynamic vNIC Connection Policy.
10. Select the Expert option to configure the LAN connectivity.
11. Click Add to add the vNIC.
12. Click Use vNIC Template in the Create vNIC window that appears.

Create vNIC

Name :

MAC Address

MAC Address Assignment: [Create MAC Pool](#)

Select MAC address assignment option.

If nothing is selected, the MAC address will be assigned from the default pool.

Use vNIC Template : Fabric ID: Fabric A Fabric B Enable Failover

VLAN in LAN cloud will take the precedence over the Appliance Cloud when there is a name clash.

VLANs

VLAN Groups

 Advanced Filter
 Export
 Print
 

Select	Name	Native VLAN
<input type="checkbox"/>	Cluster	<input type="radio"/>
<input type="checkbox"/>	cvhci_vlan20	<input type="radio"/>
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB_MGMT	<input type="radio"/>

CDN Source : vNIC Name User DefinedMTU : Pin Group : [Create LAN Pin Group](#)

OK

Cancel

- Enter an appropriate name for the vNIC to be created (**vNIC-IB-Mgmt**), select vNIC_IB-Mgmt_AB for the vNIC template, and choose the Windows-40G policy from the Adapter Policy pull-down menu.

Create vNIC



Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template :

[Create vNIC Template](#)

Adapter Performance Profile

Adapter Policy :

[Create Ethernet Adapter Policy](#)



14. Click OK to add the vNIC.
15. Click Next.
16. You move to the Storage Options section. Select the Use Connectivity Policy option for the “How would you like to configure SAN connectivity?” field.
17. Choose the Infra-SAN-Policy option from the SAN Connectivity Policy pull-down menu.

- 1 Identify Service Profile Template
- 2 Storage Provisioning
- 3 Networking
- 4 SAN Connectivity
- 5 Zoning
- 6 vNIC/vHBA Placement
- 7 vMedia Policy
- 8 Server Boot Order
- 9 Maintenance Policy
- 10 Server Assignment
- 11 Operational Policies

Create Service Profile Template

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

Simple
 Expert
 No vHBAs
 Use Connectivity Policy

SAN Connectivity Policy: <not set> [Create SAN Connectivity Policy](#)

<not set>

Domain Policies

SAN-Policy

? X

< Prev
Next >
Finish
Cancel

Note: Existing SAN policy has been used in this setup, create a new SAN connectivity policy or select no vHBAs if SAN connectivity is not required

18. Click Next.
19. You move to the Zoning Options section. Don't set any zoning options. Click Next.
20. You move to the vNIC/HBA Placement section. In the Select Placement list, leave the placement policy set to Let System Perform Placement.
21. Click Next.
22. You move to the vMedia Policy section. Leave vMedia Policy unselected.
23. Click Next.
24. You move to the Server Boot Order section. Choose the C240-Boot_SSD boot policy.

Create Service Profile Template ? ×

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: Select Boot Policy to use Create Boot Policy

The default Select Boot Policy to use profile.

- Select Boot Policy to use
- Create a Specific Boot Policy
- Boot Policies
- Boot_Policy
- C240-Boot_SSD**
- CV_Boot_Policy
- CV_boop
- CV_mirboot
- default
- diag
- hci_testbp

< Prev Next > **Finish** Cancel

25. Click Next.

26. You move to the Maintenance Policy section. Change the maintenance policy to default.

- 1 Identify Service Profile Template
- 2 Storage Provisioning
- 3 Networking
- 4 SAN Connectivity
- 5 Zoning
- 6 vNIC/vHBA Placement
- 7 vMedia Policy
- 8 Server Boot Order
- 9 Maintenance Policy
- 10 Server Assignment
- 11 Operational Policies

Create Service Profile Template ? X

Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.

⊖ Maintenance Policy

Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

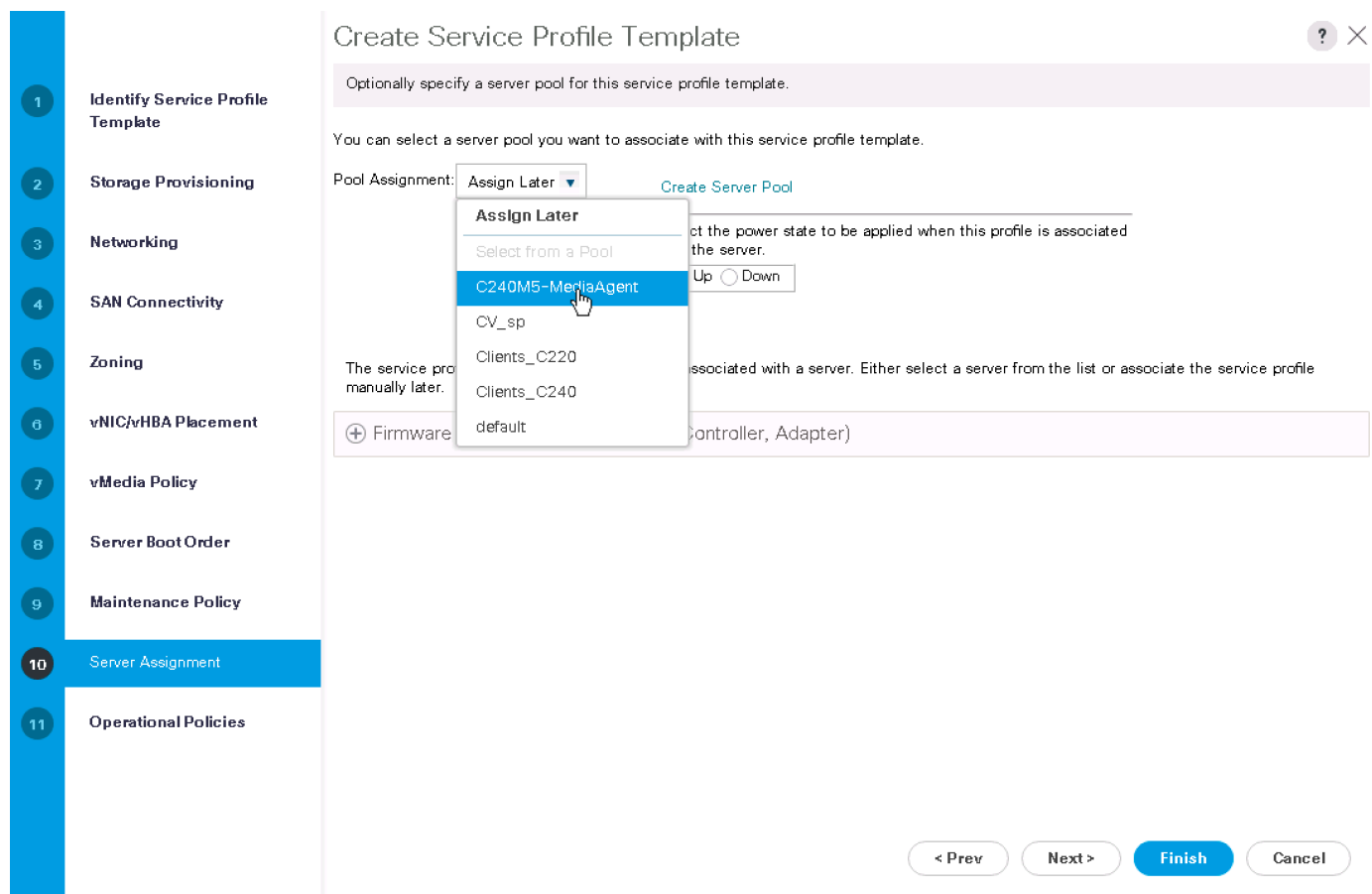
Maintenance Policy: default ▾ [Create Maintenance Policy](#)

Name	:	default	
Description	:		
Soft Shutdown Timer	:	150 Secs	
Storage Config. Deployment Policy	:	User Ack	
Reboot Policy	:	Immediate	

< Prev
Next >
Finish
Cancel

27. Click Next.

28. You move to the Server Assignment section. In the Pool Assignment list, select C240M5-MediaAgent.



Create Service Profile Template

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment: **Assign Later** [Create Server Pool](#)

Assign Later

- Select from a Pool
- C240M5-MerlaAgent**
- CV_sp
- Clients_C220
- Clients_C240
- default

The service profile is associated with a server. Either select a server from the list or associate the service profile manually later.

Firmware (Controller, Adapter)

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

29. Leave the Firmware Management at the bottom of the page as is because you will use the default settings from the Host Firmware list.
30. Click Next.
31. You move to the Operational Policies section. In the BIOS Policy list, select Host-Bios.
32. Expand Power Control Policy Configuration and select No-Power-Cap in the Power Control Policy list.

Note: The setup described here uses existing BIOS and power control policies. Create new BIOS and power control policies and select them if you are configuring a new Cisco UCS domain installation.

- 1
- Identify Service Profile Template**
- 2
- Storage Provisioning**
- 3
- Networking**
- 4
- SAN Connectivity**
- 5
- Zoning**
- 6
- vNIC/vHBA Placement**
- 7
- vMedia Policy**
- 8
- Server Boot Order**
- 9
- Maintenance Policy**
- 10
- Server Assignment**
- 11
- Operational Policies**

Create Service Profile Template ? X

Optionally specify information that affects how the system operates.

- BIOS Configuration

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile

BIOS Policy: Host-Bios ▼

+ External IPMI Management Configuration

+ Management IP Address

+ Monitoring Configuration (Thresholds)

- Power Control Policy Configuration

Power control policy determines power allocation for a server in a given power group.

Power Control Policy: No-Power-Cap ▼ [Create Power Control Policy](#)

+ Scrub Policy

+ KVM Management Policy

+ Graphics Card Policy

< Prev
Next >
Finish
Cancel

33. Click Finish to create the service profile template.

34. Click OK in the confirmation message.

Create service profiles

To create a service profile from the service profile template, complete the following steps:

1. Connect to the Cisco UCS 6332-16UP Fabric Interconnect in Cisco UCS Manager and click the Servers tab in the navigation pane.
2. Choose Service Profile Templates > root > Service Template C240-MediaAgent.
3. Right-click C240-MediaAgent and choose Create Service Profiles from Template.
4. Enter **C240-MediaAgent-0** as the service profile prefix.
5. Leave 1 set as the name suffix starting number.
6. Set **1** as the number of instances.
7. Click OK to create the service profiles.

Create Service Profiles From Template ? X

Naming Prefix : C240-MediaAgent-0

Name Suffix Starting Number : 1

Number of Instances : 1

OK

Cancel

- Click OK in the confirmation message to provision the MediaAgent service profile.

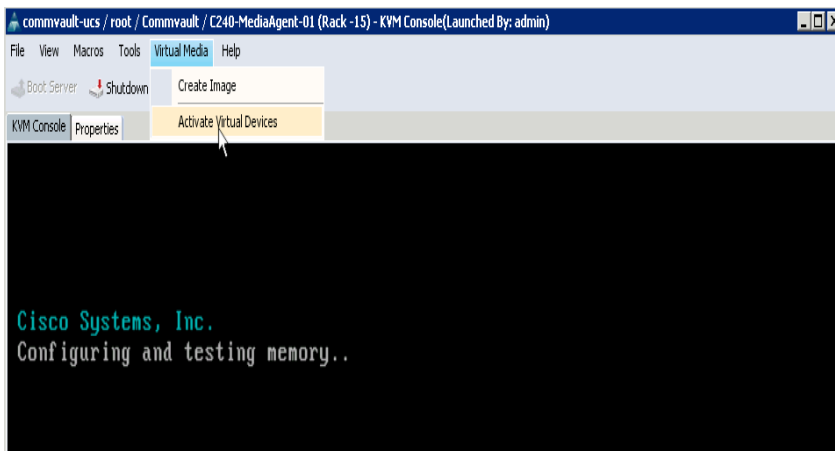
OS installation for Commvault MediaAgent server

The installation steps for the Cisco UCS C240 M5 server for MediaAgent include installing Microsoft Windows Server 2012 R2. The steps here use a Cisco UCS Manager KVM installation process from locally access vMedia mapping.

To begin the installation, open a Cisco UCS Manager KVM console from the General tab of the associated service profile of the first server to be installed. Then perform the following steps:

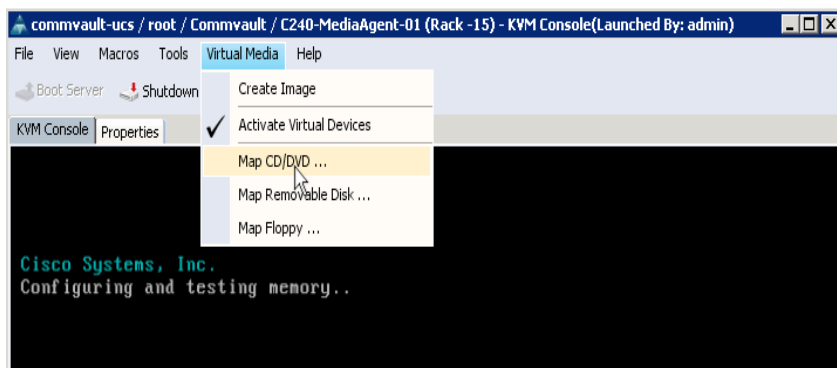
Note: For a standalone installation of the C240 server, launch the KVM console from the IMC GUI

- Click Virtual Media and choose Activate Virtual Devices from the pull-down menu.

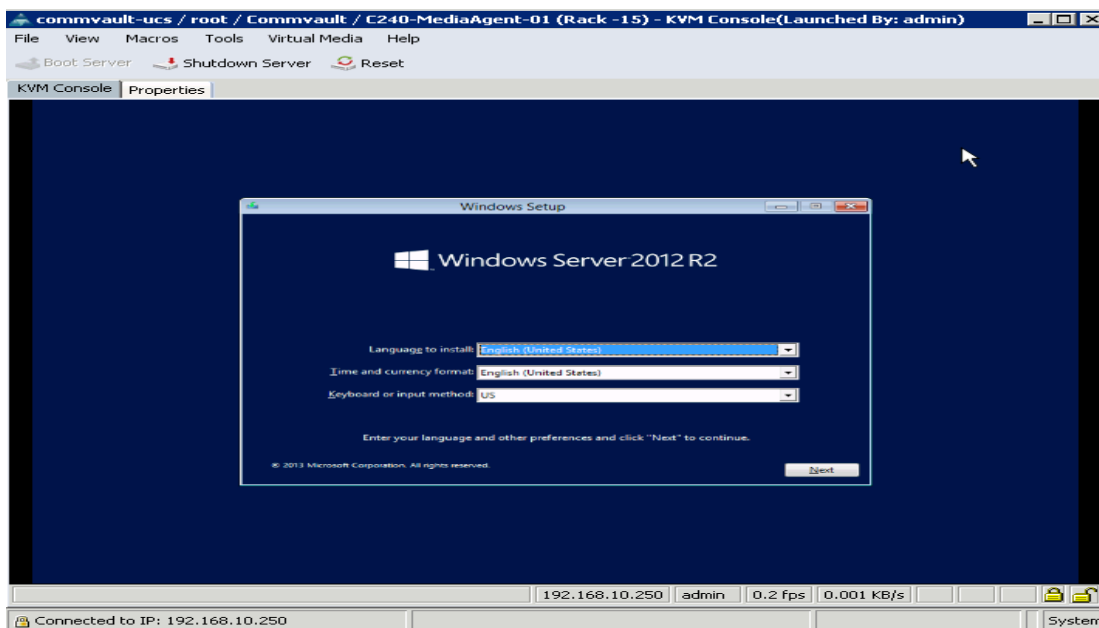


- Click Virtual Media again and choose Map CD/DVD from the pull-down menu.

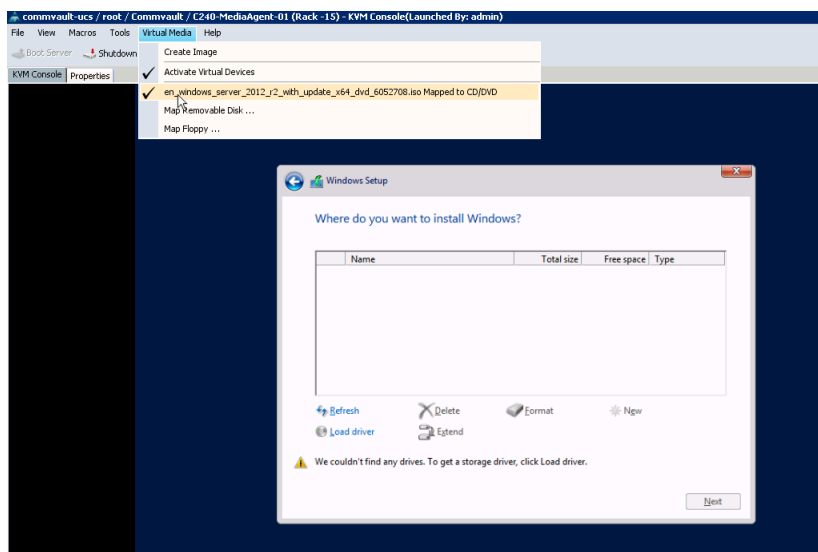
- Click Browse in the Virtual Media pop-up window and locate and select the OS installation ISO image in the pop-up window that appears. Click Open.



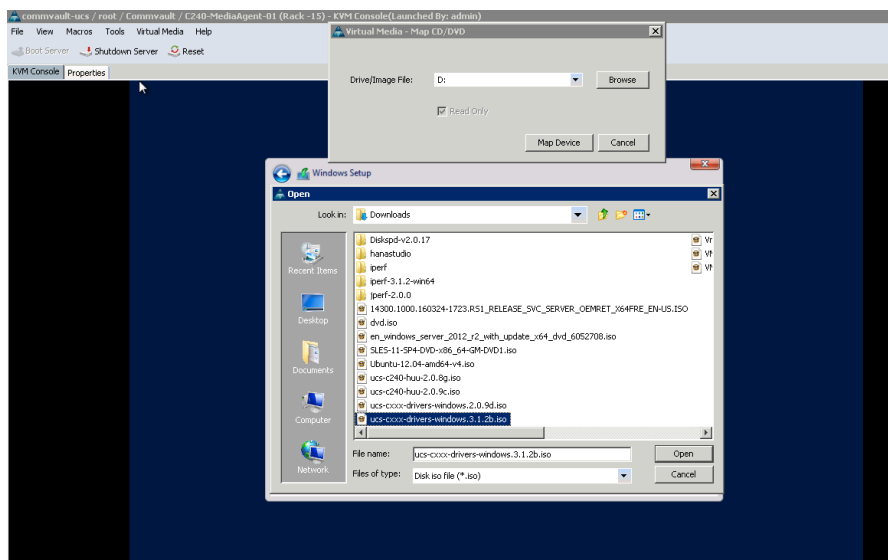
- Click Reset if the system has progressed past the boot selection menu before the Windows ISO image is mapped through KVM vMedia.
- The boot order will initiate the OS installation automatically. Click Next at the OS installation start screen.



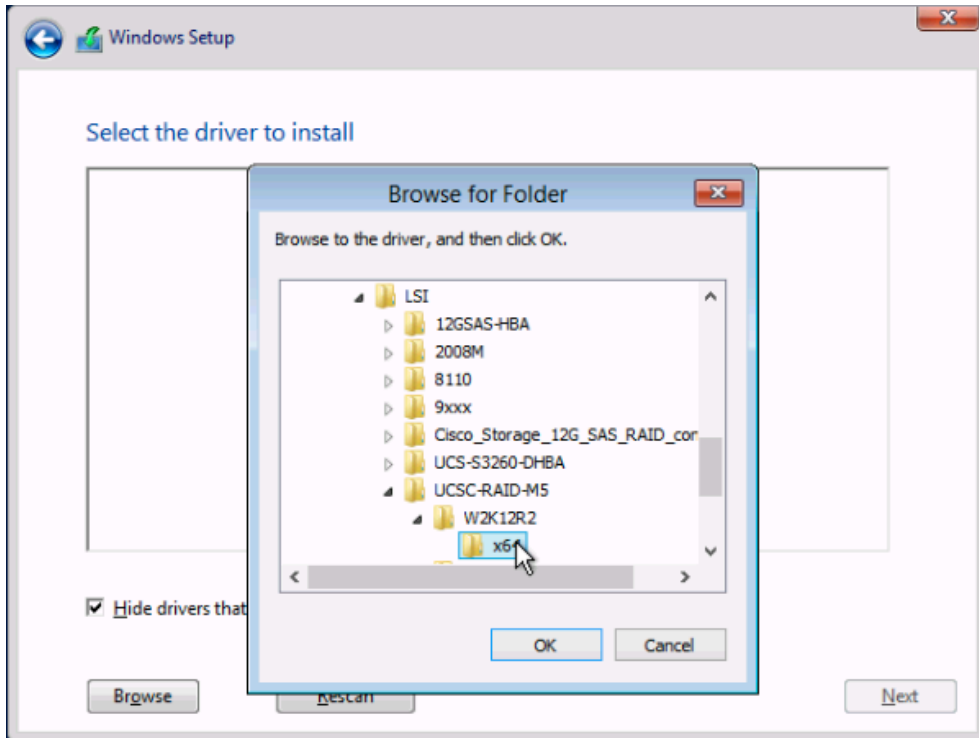
- Proceed with the installation, entering a valid Windows license key and selecting the mode (GUI mode is used in this example).
- Accept the license and select "Custom: Install Windows only (advanced)."
- When the installation destination screen appears, no suitable drives for the C240 will be displayed. Download the Windows driver ISO image from software.cisco.com at <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286281356&flowid=71443&softwareid=283853158>.
- Unmap the Windows OS installation ISO image as vMedia.



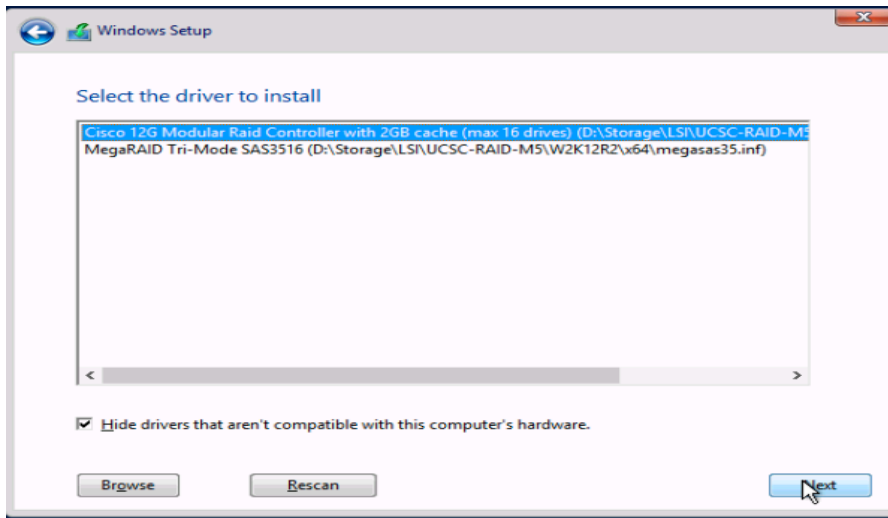
10. Click Yes to confirm the unmap drive request.
11. Reopen the Virtual Media pull-down menu, choose Map CD/DVD, and find the downloaded Cisco UCS driver ISO image using the Browse option.



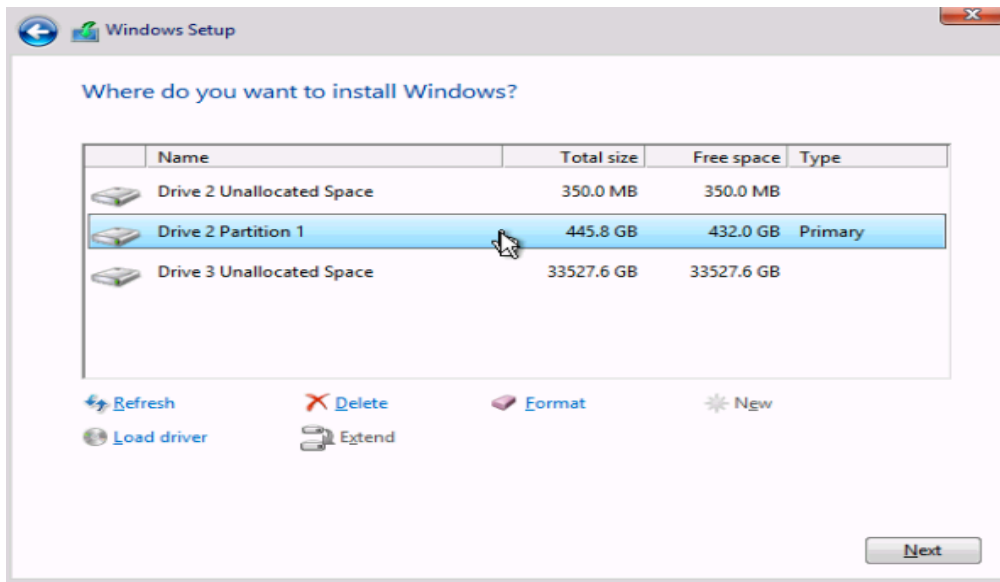
12. Click Open and choose Map Device.
13. Click Load Driver and select Browse in the pop-up window that appears.
14. Select the storage directory in the mapped CD-ROM drive.
15. Drill further down in the storage directory to LSI > UCSC-RAID-M5 > W2K12R2 > x64 and click OK.



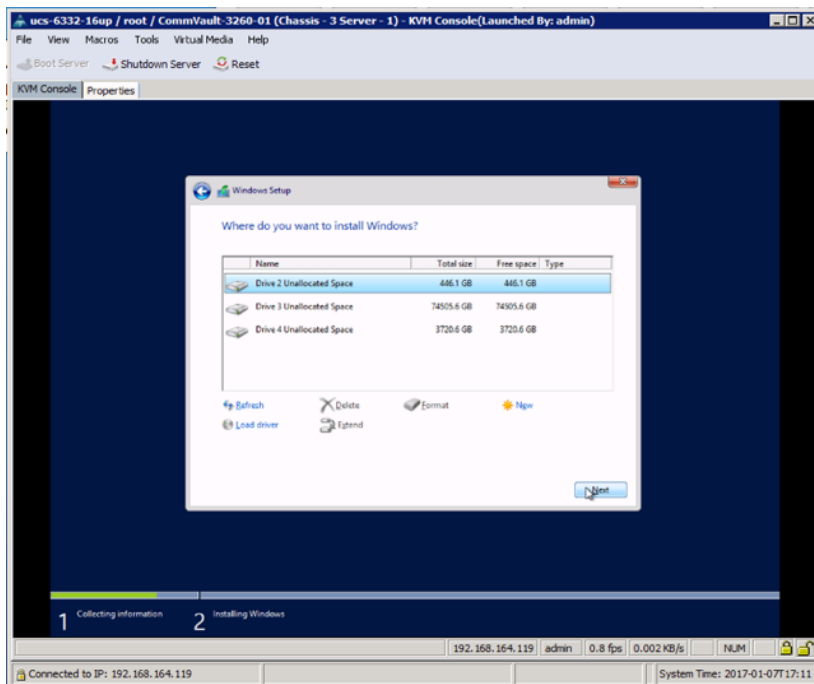
16. Select the driver that is found and click Next.



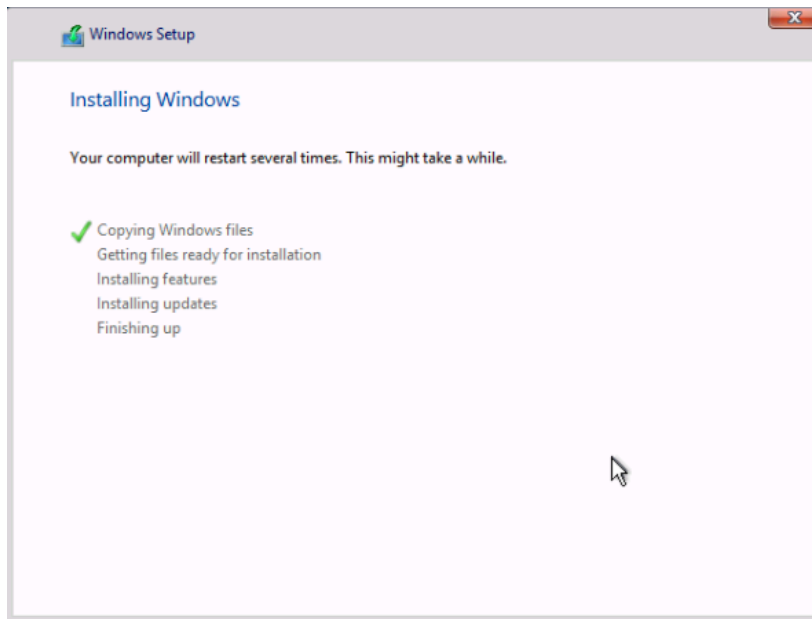
17. Select the drive on which you want to install the Windows OS and reopen the Virtual Media pull-down menu to unmap the Cisco Windows drivers ISO image.



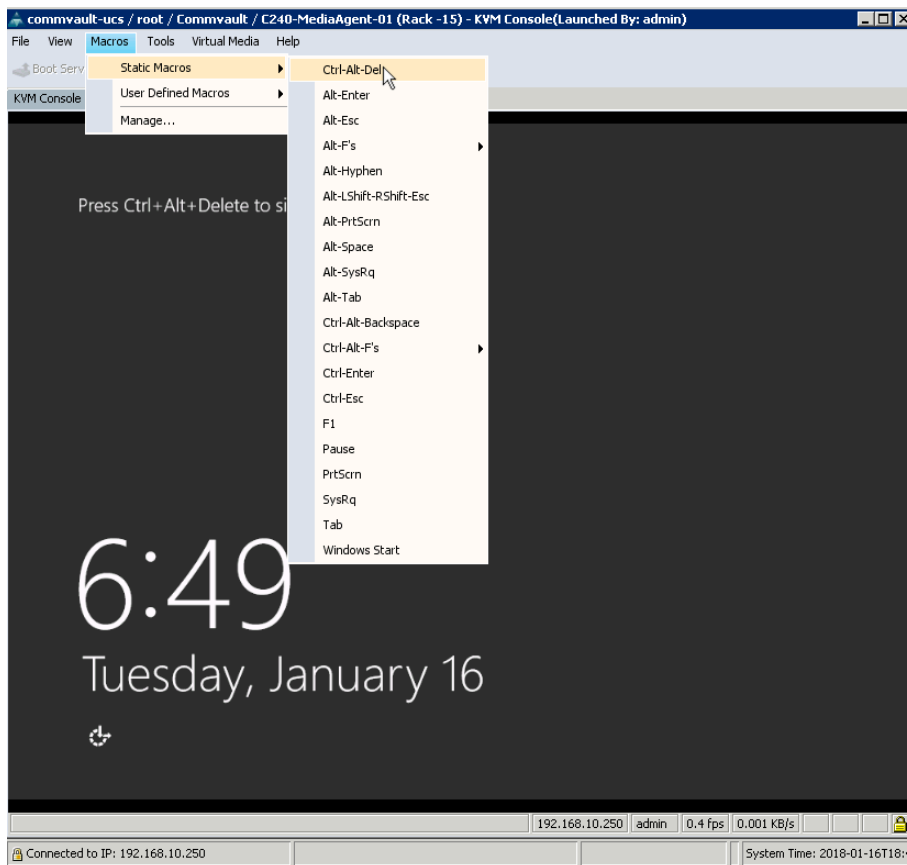
18. Click Yes to confirm the unmapping of the ISO image and reopen the Virtual Media pull-down menu to remap the Windows OS installation ISO image.
19. Click Next to begin the installation while the appropriate boot drive being selected.



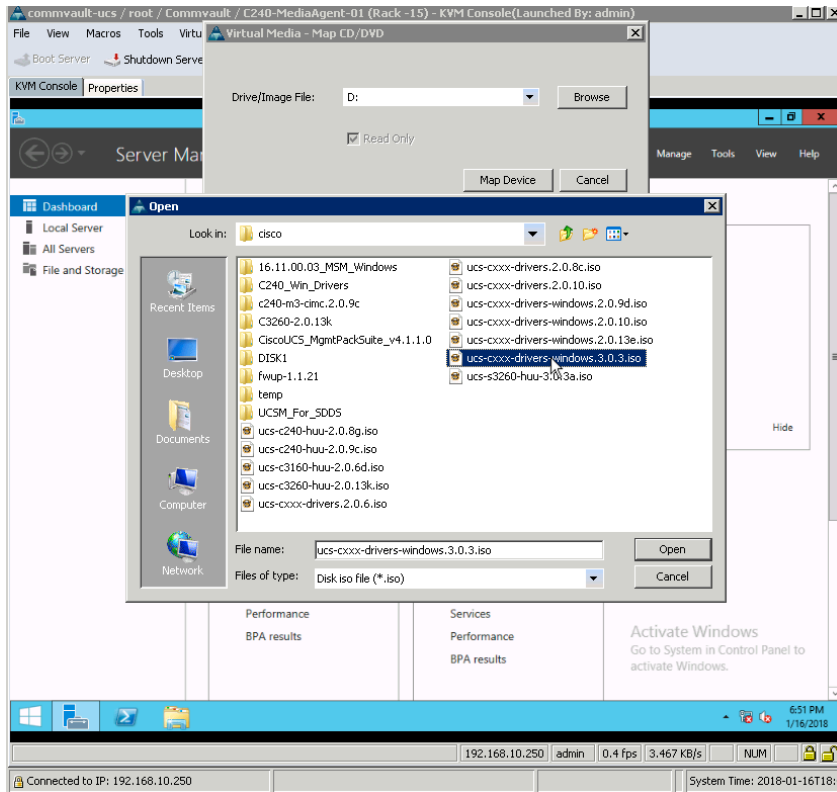
20. Wait for the Windows setup to complete.



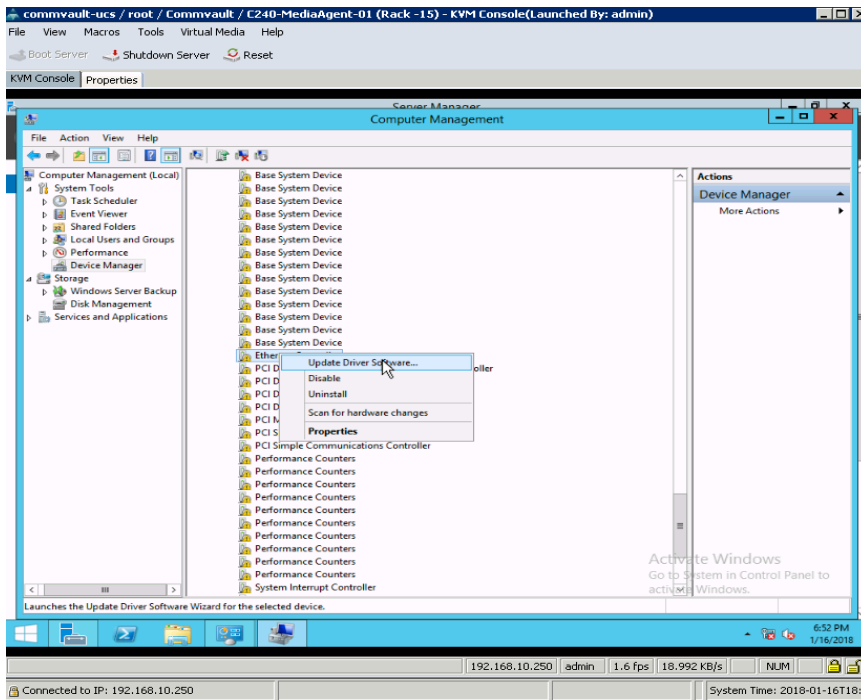
21. Unmap the Windows OS installation ISO image after the installation is complete.
22. Provide an administrator password and click Finish.
23. Use the static macro for Ctrl-Alt-Del to log in to the system.



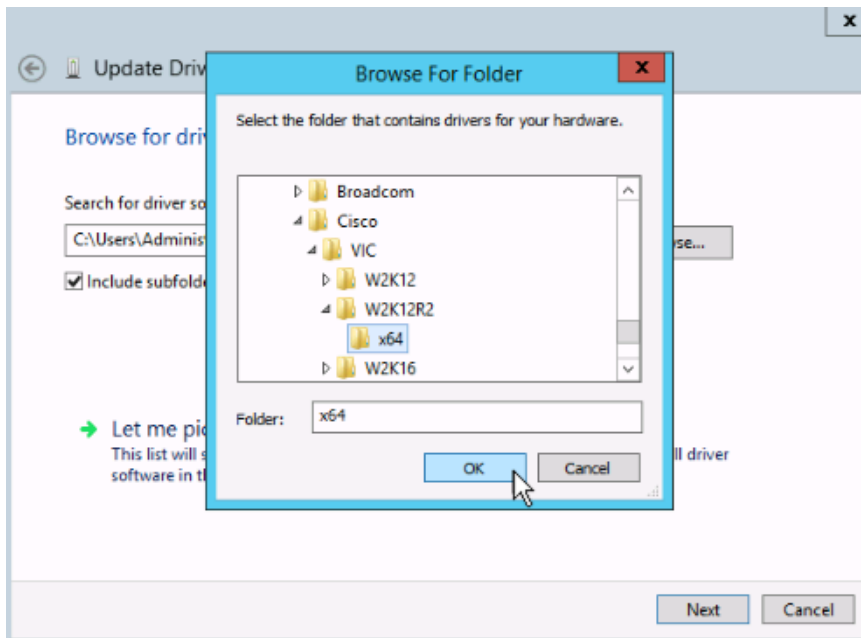
24. Reopen the Virtual Media pull-down menu and go through the steps to remap the Cisco UCS drivers for the Windows ISO image.



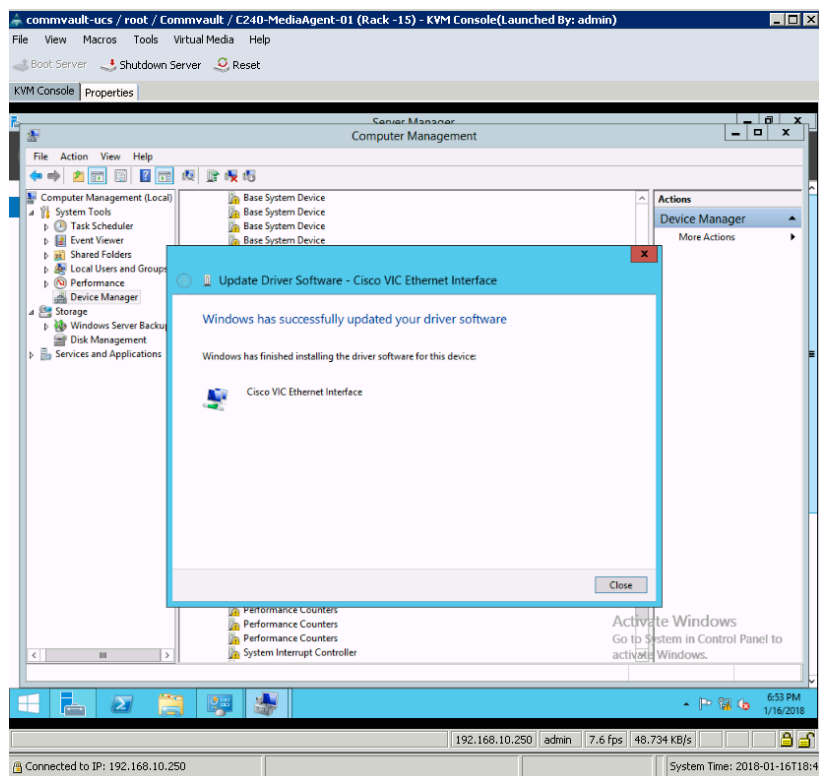
25. Open Device Manager and find the unidentified Ethernet controller device under Other Devices. Right-click and choose Update Driver Software.



26. Select “Browse my computer for driver software” in the pop-up window that appears.
27. Click Browse in the Update Driver Software – Ethernet Controller window and drill down from the mapped CD drive to Network > Cisco > VIC > W2K12R2 > x64 and click OK.



28. Click Next to update the driver.



29. Update the Fibre Channel drivers if SAN connectivity is needed for the MediaAgent server.
30. Click Close. With the Device Manager still open, scroll down within Other Devices and find an entry for the first Fibre Channel controller. Right-click and choose Update Driver Software.
31. Repeat this process for the Ethernet controller. Select “Browse my computer for driver software.”
32. Select Browse and drill down from the mapped CD drive to Storage > Cisco > VIC > W2K12R2 x64 and click OK.
33. Click Next to update the driver.
34. Click Close.
35. Repeat these steps for the second Fibre Channel controller.
36. Click Close.
37. Open Windows File Explorer and drill down from the mapped CD drive to Chipset > Intel > [C240M5] > W2K12R2 and open the SetupChipset application.
38. Click Next at the Welcome window, click Accept to get past the End-User License Agreement (EULA), and click Install.
39. When you are finished, click Restart Later.
40. Configure the network interface with an IP address and enable Remote Desktop.
41. Complete the OS updates and join the OS to an appropriate domain.
42. Disconnect the vMedia as the system reboots.

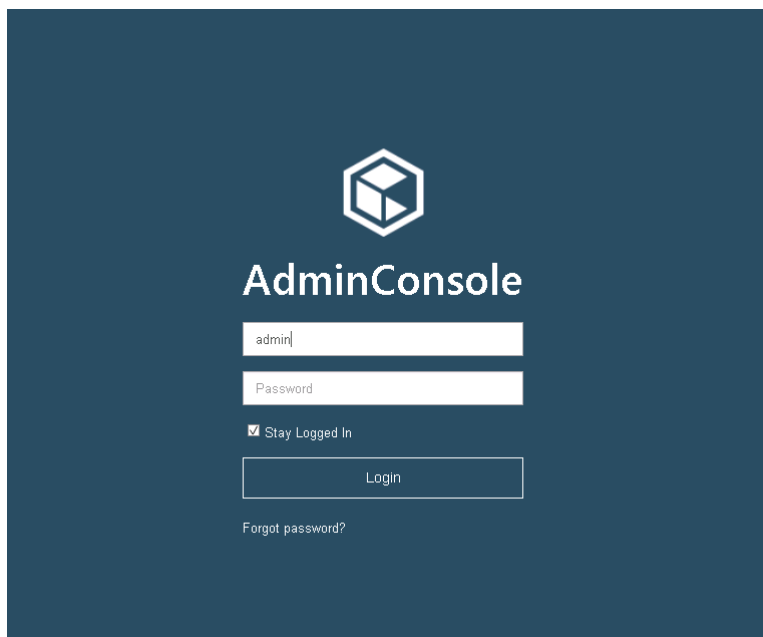
Commvault MediaAgent installation and configuration

To deploy the MediaAgent software on the Cisco servers, use the following steps for remote deployment of the software:

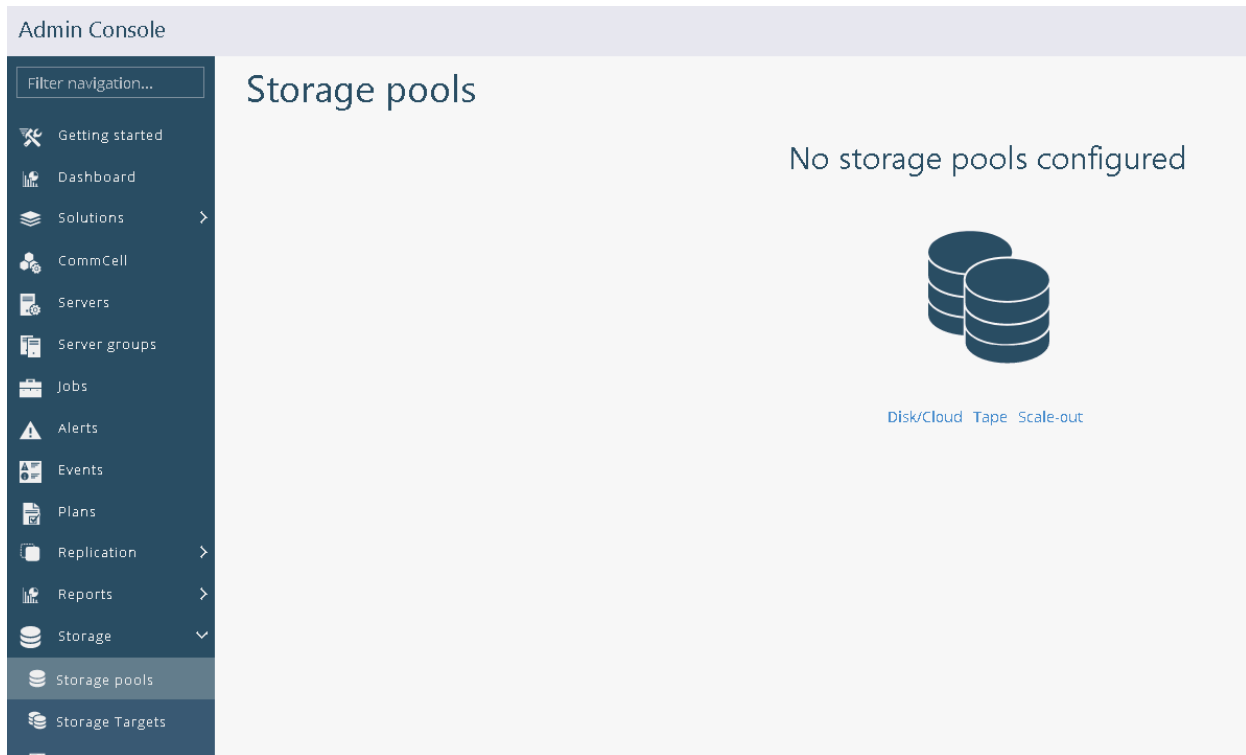
1. From the CommCell Console ribbon, on the Tools tab, click Add/Remove Software. Then choose Install Software from the drop-down menu.
2. The Install Wizard will appear. Click Next.
3. On the “Select the computer’s operating system” page, select the OS and click Next.
4. On the “Select how to discover the computers for installing the software” page, click Next.
5. On the Select the computer’s operating system” page, select the OS and click Next.
6. On the “Enter the host names of the computers” page, enter the host names or IP addresses of any Cisco servers that will host the MediaAgent role. Then click Next.
7. On the Enter Account Information page, enter credentials for a user with local administrator or root privileges on the server and click Next.
8. On the Select Package(s) to Install page, select the MediaAgent package and click Next.
9. On the Optional Settings page, select the “Index cache to this folder” checkbox and enter `I:\indexcache` in the Index Cache path field. Then click Next.
10. On the Firewall Configuration page, click Next.
11. On the Please Select When To Run The Job page, click Next.
12. On the Summary page, click Finish. An install software job will be initiated. Monitor this job in the job controller window.

After the MediaAgent software is installed, you need to create the storage pool. This process will configure the disk library and create a storage policy so that clients can back up their data. More than one storage pool may be required depending on the design. For the drive dedicated for the disk library, format the drive with an OS block size of 64 KB.

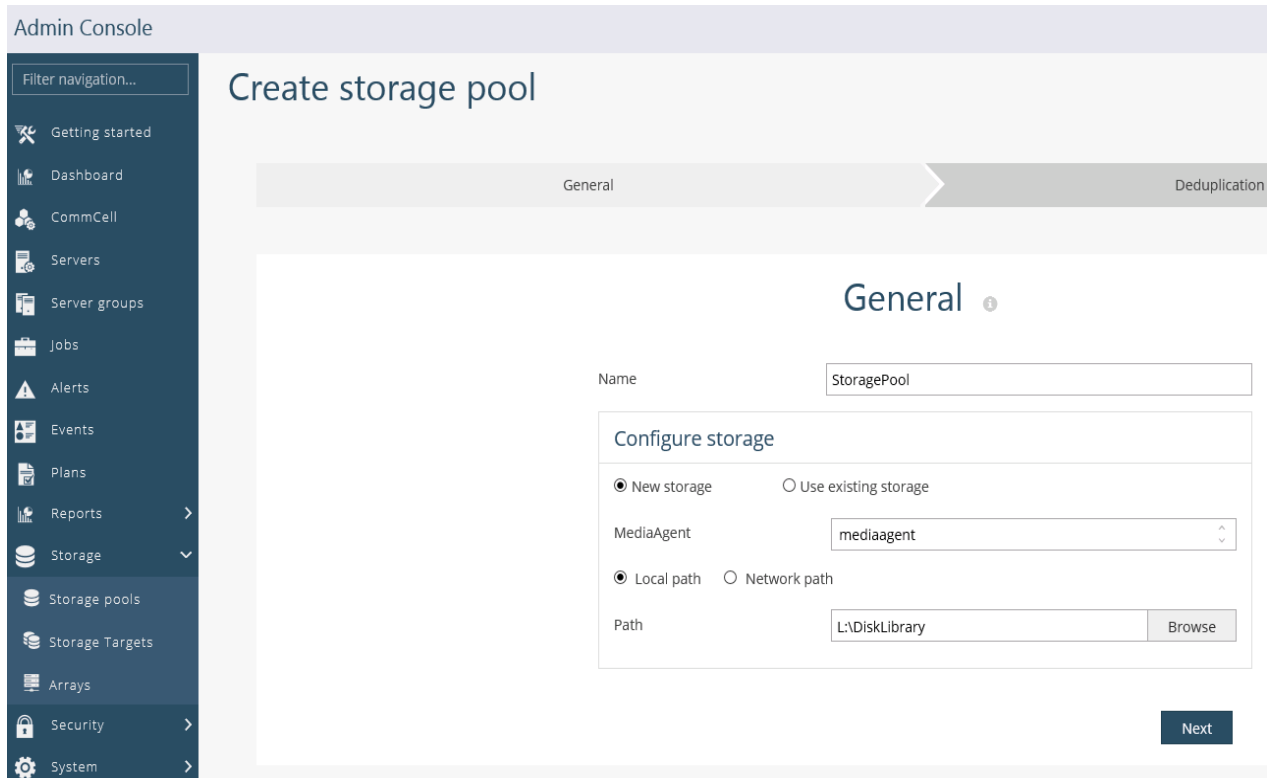
1. Log on to AdminConsole.



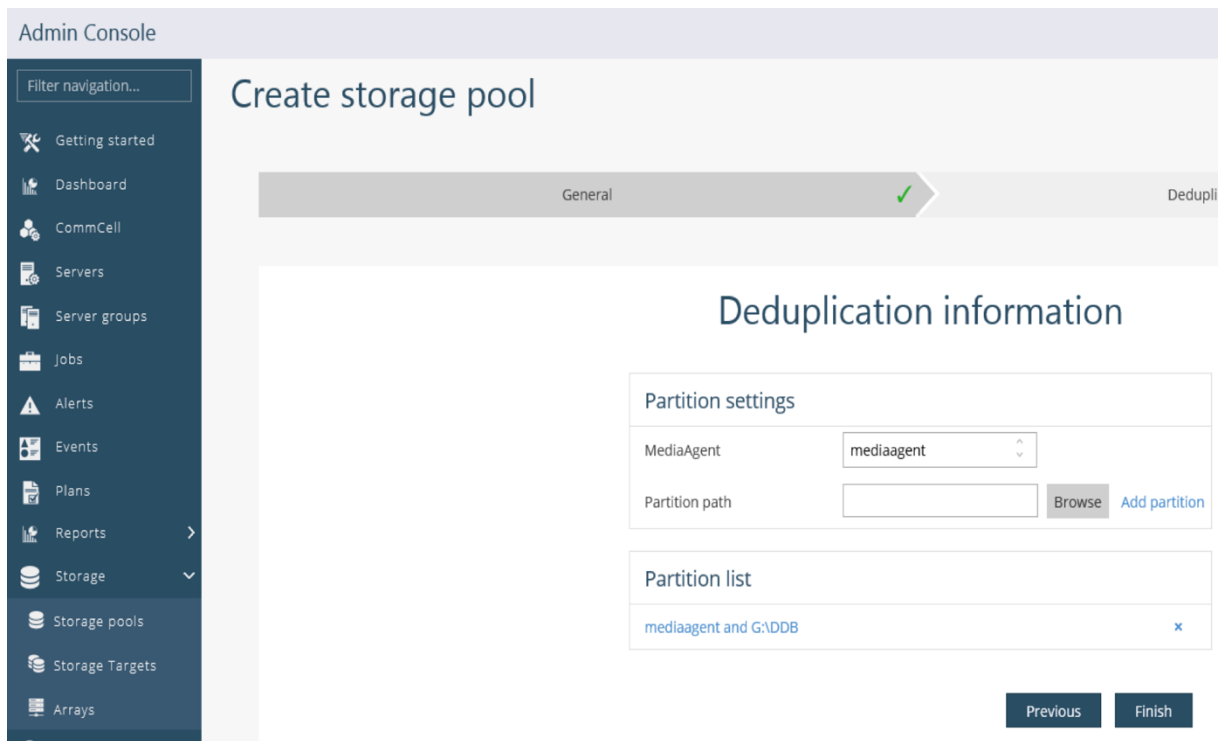
- In the left pane, expand Storage, select “Storage pools,” and then select Disk/Cloud.



- Give the storage pool a name and select MediaAgent and the path for the disk library. Then click Next.



- Select the same MediaAgent again and select the path for the deduplication database. Click Add Partition and then click Finish.



The screenshot shows the 'Admin Console' interface for creating a storage pool. The main heading is 'Create storage pool'. A progress bar at the top indicates the 'General' step is completed (marked with a green checkmark) and the 'Deduplication information' step is currently active. The 'Deduplication information' section contains two main areas: 'Partition settings' and 'Partition list'. In 'Partition settings', the 'MediaAgent' is set to 'mediaagent' and the 'Partition path' is empty, with a 'Browse' button and an 'Add partition' link. The 'Partition list' shows a single entry: 'mediaagent and G:\DDB'. At the bottom of the wizard, there are 'Previous' and 'Finish' buttons.

The disk library is now ready for use.

For more information

For additional information, see the following:

- Cisco UCS S3260 Storage Server:
<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-s-series-storage-servers/index.html>
- Cisco UCS 6000 Series Fabric Interconnects:
<http://www.cisco.com/c/en/us/products/servers-unified-computing/fabric-interconnects.html>
- Cisco UCS Manager:
<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-manager/index.html>
- Achieve Optimal Network Throughput on the Cisco UCS S3260 Storage Server (Cisco white paper):
http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-s-series-storage-servers/Whitepaper_c11-738722.html
- Commvault:
<https://www.commvault.com/solutions/by-function/data-protection-backup-and-recovery>

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)